LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 7/2166**
7. Wahlperiode **17.05.2018**

UNTERRICHTUNG

durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Dreizehnter Tätigkeitsbericht gemäß § 33 Absatz 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V)

Achter Tätigkeitsbericht gemäß § 38 Absatz 1 Bundesdatenschutzgesetz (BDSG)

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

Berichtszeitraum: 1. Januar 2016 bis 31. Dezember 2017

Zugeleitet mit Schreiben des Landesbeauftragten für Datenschutz und Informationsfreiheit vom 15. Mai 2018

Vorwort

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat dem Landtag und der Landesregierung für jeweils zwei Kalenderjahre einen Bericht über seine Tätigkeit vorzulegen.
Der Dreizehnte Tätigkeitsbericht gemäß § 33 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V), der Achte Tätigkeitsbericht gemäß § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) und der Sechste Tätigkeitsbericht nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) umfassen den Zeitraum vom 1. Januar 2016 bis zum 31. Dezember 2017. Da es bei etlichen Sachverhalten fachliche Überschneidungen gibt, sind die Beiträge nach dem DSG M-V und nach dem BDSG nicht separat aufgeführt, weil die Themen häufig im Zusammenhang zu betrachten sind.
Die hier dargestellten Vorgänge sollen einen Eindruck von der breit gefächerten Tätigkeit der Behörde als Beratungs-, Aufsichts- und Kontrollbehörde vermitteln. Einige Beiträge schließen an Sachverhalte aus den Tätigkeitsberichten der vorherigen Berichtszeiträume an. Insofern könnte es nützlich sein, in dem einen oder anderen Fall noch einmal auf diese Berichte zurückzugreifen.

Heinz Müller
Landesbeauftragter für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern

Inhaltsverzeichnis

		Seite
0	Einleitung	6
1	Empfehlungen	7
1.1	Zusammenfassung aller Empfehlungen	7
1.2	Umsetzung der Empfehlungen des Zwölften Tätigkeitsberichtes	8
2	Vorsitz der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)	15
2.1	Turnusmäßige Sitzungen	15
2.2	Zusammenarbeit mit BMI und IMK	17
2.3	Der 11. Europäischer Datenschutztag	17
3	Neuer Europäischer Rechtsrahmen im Datenschutz	19
3.1	Neues EU-Recht im Datenschutz - die europäische Datenschutz-Grundverordnung (DS-GVO)	19
3.1.1	Ausstattung der Dienststelle	22
3.2	Die JI-Richtlinie	25
3.3	Lehr-Schulungs-und Informationsveranstaltungen zum Europäischen Datenschutzrecht	26
4	Datenschutz und Bildung	27
4.1	Medienbildung/Medienkompetenzvermittlung	29
4.1.1	Projekte „Medienscouts M-V“ und „TEO - Protect Privacy“	30
4.1.2	Netzwerk „Medienaktiv M-V“	32
4.1.3	Kooperationsvereinbarung zur Medienkompetenzförderung	33
4.1.3.1	Arbeitsgruppe „*KITA*“/AG Frühkindliche Medienbildung	34
4.1.4	Kampagne „Medien- Familien-Verantwortung“	35
4.1.5	Ausblick/Fazit	36
5	Technik und Organisation	37
5.1	Neue Technologien	37
5.1.1	Das Standard-Datenschutz-Modell	37
5.1.2	E-Government mit modernen Kommunikationsstandards	40
5.1.3	Datenschutz im Internet der Dinge	41
5.1.4	Infrastrukturenkomponenten nicht vergessen	43
5.1.5	elektronische Akte (eAkte)	44
5.1.6	Algorithmen	46
5.2	Kommunikation/neue Medien	47
5.2.1	TLSA/DANE - Internetdienste besser sichern	47
5.2.2	Neugestaltung des „Virtuellen Datenschutzbüros“	48
5.3	Videoüberwachung	49
5.3.1	Einsatz einer Rettungsdrohne durch das DRK	49
5.3.2	Einsatz von Drohnen durch eine Freiwillige Feuerwehr	50
5.3.3	„Nachbarschaftliche“ Videoüberwachung	51
5.3.4	Videoüberwachung in einem Jugendfreizeittreff	52
5.3.5	Videoüberwachung an Schulen	53

Seite

6	Datenschutz in verschiedenen Rechtsgebieten	54
6.1	Rechtswesen	54
6.1.1	Verletzung der Auskunftspflicht kann teuer werden	54
6.1.2	Einscannen von Personalausweisen und Pässen bei Schiffsreisen	54
6.1.3	„Strafzettel“ auf privatem Parkplatz	55
6.2	Polizei/Ordnungswesen	56
6.2.1	Bodycams bei der Polizei in Mecklenburg-Vorpommern	56
6.2.2	Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz (BKAG)	57
6.3	Justiz	59
6.3.1	Datenschutz in den Justizvollzugsanstalten in Mecklenburg-Vorpommern	59
6.4	Kommunales	59
6.4.1	Ratsinformationssysteme auf Tablets	59
6.4.2	Datenerhebung durch kommunale Recyclinghöfe	63
6.4.3	Veröffentlichungen von Unterschriftenlisten bei Einwohneranträgen und Bürgerbegehren im Internet	64
6.4.4	Umgang mit Traueranzeigen	65
6.5	Soziales/Arbeitnehmerdatenschutz	65
6.5.1	Landkreis verlangt vom Sozialhilfeträger eine Erklärung zur Offenlegung der Einkommens- und Vermögensverhältnisse	65
6.6	Gesundheitswesen	67
6.6.1	Entwicklung des Krebsregisterrechts im Berichtszeitraum	67
6.6.2	Zusammenfassung verschiedener Beratungen im Telemedizinbereich	68
6.6.3	Fragebogenaktion zum Stand der Anpassung der Praxisorganisation an die Datenschutz-Grundverordnung	68
6.6.4	Befundanforderungen durch das Landesamt für Gesundheit und Soziales	69
6.6.5	Umgang mit Patientenakten/Patientendokumentationen	69
6.7	Finanzwesen	70
6.7.1	Kopieren von Personalausweisen beim Schrotthandel als Nachweis für das Finanzamt?	70
6.7.2	Support für Steuerverfahren ohne Rechtsgrundlage	71
6.8	Bildung	72
6.8.1	Datenschutz in den Schulen	72
6.8.2	Das Schul-Cloud-Projekt des Hasso-Plattner-Instituts	74
7	IT-Planungsrat	76
7.1	Turnusmäßige Sitzungen des IT-Planungsrates	76
7.2	Ausgewählte Aspekte der Tätigkeit des IT-Planungsrates	76
8	Arbeitskreis „Technische und organisatorische Datenschutzfragen“	78
8.1	Turnusmäßige Sitzungen	78
8.2	Workshop	80
8.3	Technology Subgroup - Zusammenarbeit auf europäischer Ebene	81
9	Öffentlichkeitsarbeit	82

Seite

10	Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V	82
10.1	Auswirkungen der EU-DSGVO auf die Informationsfreiheit in Mecklenburg-Vorpommern	83
10.2	Grundsatzpositionen der Informationsfreiheitsbeauftragten der Länder gegenüber der Bundespolitik	84
10.3	Das Informationsfreiheitsgesetz - weiterer Novellierungsbedarf besteht	85
10.4	Frühzeitige Herausgabe von Informationen über Meistbietenden	87
10.5	Verweigerung der Herausgabe eines Pachtvertrages an Ferienhauseigentümerin	88
10.6	Transparenz beim NDR	89
10.7	Anwendbarkeit des IFG nach Abschluss des Vergabeverfahrens im Unterschwellenbereich	89
10.8	Bauvorlagen als Betriebs- oder Geschäftsgeheimnisse	91
11	Abkürzungsverzeichnis	93
12	Stichwortverzeichnis	96

0 Einleitung

Der Berichtszeitraum war geprägt durch eine weiterhin sehr rasante technische Entwicklung im Bereich der Datenverarbeitung und der elektronischen Kommunikation. Zunehmend finden Techniken zur Verarbeitung sehr großer Datenmengen, die in hoher Geschwindigkeit erzeugt werden und aus sehr unterschiedlichen Quellen stammen, Anwendung in unserem Alltagsleben. Das Schlagwort der „Digitalisierung“ klassifiziert die gesellschaftliche Entwicklung nicht nur der Industriestaaten. Die Bedeutung sozialer Netzwerke wächst ständig.

Wir haben uns daran gewöhnt, dass der Präsident der Vereinigten Staaten seine Kommunikation mit der Öffentlichkeit häufig über soziale Medien gestaltet. Auch bei uns im Land nutzen die Verwaltung des Landtages und Teile der Landesregierung inzwischen „Social Media“ für die eigene Kommunikation. „Smart Home“ wird für immer breitere Kreise interessant. Gesetzliche Regelungen für das automatisierte Verfahren schaffen einen Rechtsrahmen für eine technologische Entwicklung, die unser Alltagsleben stark verändern wird, wobei nur am Rande diskutiert wird, welche Mengen an Daten hierbei anfallen und verarbeitet werden. Methoden der technologischen Gesichtserkennung und der Verarbeitung biometrischer Daten werden nicht mehr nur bei Ausweispapieren, sondern in vielfältiger Weise genutzt.

Die technischen Möglichkeiten finden in den unterschiedlichsten Bereichen von Wirtschaft und Verwaltung Anwendung, beispielsweise beim Scoring von Bankkunden. Von besonderer Bedeutung war in den letzten zwei Jahren der Wunsch breiter Teile der Politik, moderne Techniken auch für eine Verbesserung der inneren Sicherheit einzusetzen. Dabei darf bei vielen der beschlossenen Maßnahmen durchaus die Frage gestellt werden, inwieweit der angestrebte Zweck hier tatsächlich erreicht wird. Vor allem aber stellt sich die Frage, inwieweit solche Maßnahmen über das vernünftige Maß hinaus in das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger eingreifen. Beispielhaft für diese Diskussion steht die Debatte um eine Ausdehnung der Videoüberwachung von öffentlichen und öffentlich zugänglichen Räumen.

Im Bereich des Datenschutzrechts war das prägende Ereignis die Verabschiedung der Europäischen Datenschutz-Grundverordnung (*EU-DSGVO*) durch die Gremien der Europäischen Union im Frühjahr des Jahres 2016. Diese Verordnung, ab Mai 2016 in Kraft und nach einer Übergangszeit von zwei Jahren ab Mai 2018 in allen Mitgliedsstaaten der Europäischen Union unmittelbar geltendes Recht, vereinheitlicht das Datenschutzrecht in Europa und setzt für alle Mitgliedsstaaten Maßstäbe. Nationales Recht muss an die DSGVO angepasst werden.

Der Bund hat einen wesentlichen Teil seiner gesetzgeberischen Aufgaben mit der Verabschiedung des neuen Bundesdatenschutzgesetzes (*BDSG*) erledigt. Die Anpassung einer großen Zahl weiterer Bundesgesetze ist in Arbeit. Im Land Mecklenburg-Vorpommern ist zum Zeitpunkt des Abschlusses dieses Berichtes die entsprechende gesetzgeberische Arbeit in vollem Gange. Unter anderem wird die Landesverfassung novelliert, ein neues Landesdatenschutzgesetz ist zu verabschieden und zahlreiche weitere Landesgesetze sind anzupassen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist von der Landesregierung, die für diese Gesetze Entwürfe erarbeitet, in vielfältiger Weise in die Beratungen einbezogen worden. Wir haben es als eine unserer zentralen Aufgaben angesehen, hier unseren Sachverstand in die Beratungen einzubringen und auf datenschutzfreundliche Regelungen zu drängen. Das Ergebnis der Gesetzgebungsarbeit bleibt abzuwarten.

Die wachsenden Aufgaben der Behörde, insbesondere schon im Vorfeld von der EU-Datenschutz-Grundverordnung erzeugt, sind mit den vorhandenen Kräften nicht zu bewältigen. Im Berichtszeitraum wurden fünf befristete Stellen in unbefristete umgewandelt, sodass hier entsprechende Arbeitsverträge geschlossen werden konnten. Dieses war eine wichtige Weichenstellung für unsere künftige Arbeit. Der Antrag auf weitere dringend benötigte Stellen ist zum Zeitpunkt der Abfassung dieses Berichtes noch nicht entschieden.

Wichtige interne Personalie war der Wechsel des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern. Nach dem Ablauf der Amtszeit von Reinhard Dankert im Dezember 2016 wurde Heinz Müller neuer Landesbeauftragter.

1 Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

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, siehe Punkt 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, siehe Punkt 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, siehe Punkt 5.1.6.

1.2 Umsetzung der Empfehlungen des Zwölften Tätigkeitsberichtes

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 12. TB
1	Wir halten an unserer Empfehlung an die Kommunen aus dem Elften Tätigkeitsbericht fest, die Vorgaben der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ umzusetzen, und erwarten, dass sie für Verfahren zur automatisierten Verarbeitung personenbezogener Daten die Grundschutzmethodik des BSI in vollem Umfang anwenden. Die „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ und der Leitfaden „Informations-Sicherheits-Management-System in 12 Schritten“ sind geeignete Hilfsmittel auf dem Weg dazu.	Die Landesregierung verweist darauf, dass die Anwendung der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ im Landtag, in den Arbeitsgremien sowie in mehreren gemeinsamen Veranstaltungen umfassend thematisiert wurde. Über diese Leitlinie hinaus, insbesondere bei den ebenenübergreifenden IT-Verfahren sowie bei der Absicherung der gemeinsam genutzten Kommunikationsinfrastruktur (CN LAVINE), soll die Grundschutzmethodik des BSI verbindlich angewendet werden. Flankierend hierzu strebt das IM den landeseinheitlichen Einsatz eines ISMS-Werkzeuges an. Darüber hinaus sollen die Kommunen auch in den gemäß der Leitlinie geforderten Aufbau des Informationssicherheitsmanagements und des Landes-CERT eingebunden werden.	3.3
2	Wir fordern daher die Landeregierung auf, sich für die folgenden Gestaltungsprinzipien bei Bürgerkonten einzusetzen. - Es muss auch künftig möglich sein, Verwaltungsdienstleistungen anonym und somit ohne Anmeldung an einem Bürgerkonto zu nutzen, sofern identifizierende Daten nicht erforderlich sind.	Die Landesregierung verweist darauf, dass die Konzeption zukünftiger Servicekonten (vormals Bürgerkonten) im IT-Planungsrat die rechtlichen Rahmenbedingungen berücksichtigt. Dazu gehören auch Aspekte des Datenschutzes. Das Innenministerium wird die Empfehlungen des LfDI in die Überlegungen zur Ausgestaltung von Servicekonten einbeziehen.	3.5

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 12. TB
	- Bürgerinnen und Bürger müssen die Wahlmöglichkeit haben, etwa bei einmaliger Inanspruchnahme einer Verwaltungsdienstleistung ihre identifizierenden Daten nur temporär im Bürgerkonto zu hinterlegen. - Entscheiden sich Nutzerinnen und Nutzer, Daten dauerhaft in einem permanenten Bürgerkonto zu speichern, muss jederzeit nachvollziehbar sein, wer zu welchem Zweck auf diese Daten zugreift. - Auf Wunsch der Nutzerinnen und Nutzer muss es jederzeit möglich sein, das Bürgerkonto und alle dort gespeicherten Daten zu löschen. - Insbesondere durch technische Maßnahmen muss die oben beschriebene Möglichkeit der Verknüpfung einzelner Nutzeraktivitäten zu einem umfassenden Nutzungsprofil ausgeschlossen werden.		
3	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 Landesregierung beabsichtigt bei der Planung, Einrichtung und dem Betrieb von IT-Verfahren zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, neben der Vorgehensweise und den Maßnahmen aus dem BSI IT-Grundschutz, insbesondere auch auf den Einsatz des SDM hinzuwirken.	4.1.1

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 12. TB
4	Wir empfehlen unserer Landesregierung schon jetzt, die im Trusted-Cloud-Projekt entwickelten Methoden und Unterlagen bei der Auswahl von Cloud-Diensten zu nutzen, um die Datenschutzkonformität von Cloud-Infrastrukturen bewerten zu können.	Die Landesregierung verweist darauf, dass sie die Methoden und Unterlagen des Trusted-Cloud-Projekts, bei der Erstellung der künftigen IT-Landesstandards als Anlage zu den IT-Richtlinien gemäß des E-Government-Gesetzes berücksichtigen wird.	4.1.2
5	Wir empfehlen den Behörden in unserem Land, den Standard XTA 2.1 in Verbindung mit OSCI-Transport zur sicheren Kommunikation zwischen Behörden einzusetzen.	Die Landesregierung verweist darauf, dass bei den E-Government-Verfahren grundsätzlich das OSCI-Transport-Protokoll eingesetzt wird. Eine Entscheidung zur Nutzung des sicheren OSCI-Transportprotokolls trifft der jeweilige Fachverfahrensverantwortliche entsprechend dem ermittelten Schutzbedarf der Daten. Zudem wird aktuell das „Elektronischen Gerichts-und Verwaltungspostfach“ (EGVP) in allen Landesbehörden eingerichtet, um die Nutzung einer, auch Ende-zu-Ende-, Verschlüsselung für die Fachverantwortlichen und Nutzer in der Landesregierung zu erleichtern.	
6	Wir empfehlen den Anwendern aus Wirtschaft und Verwaltung in unserem Land, diese Orientierungshilfe zu beachten.	Die Landesregierung begrüßt die Orientierungshilfe und wird sie weiterhin entsprechend berücksichtigen. Relevante Datenträger werden nach der DIN 66399 seit deren Gültigkeit vernichtet.	

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 12. TB
7	Wir empfehlen der Landesverwaltung, auf die Durchsetzung der oben genannten Maßnahmen zu dringen. Dem Landtag empfehlen wir, die zu ihrer Durchsetzung gegebenenfalls nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen	Die Landesregierung verweist darauf, dass im Kontext mit der Gewährleistung der Vertraulichkeit, der Integrität und der Authentizität der Kommunikationsinfrastruktur der Landesverwaltung, das Innenministerium die empfohlenen Maßnahmen berücksichtigen wird. Hierbei wird insbesondere der Fokus auf die Förderung der Vertraulichkeit informationstechnischer Systeme durch BSI-Zertifizierungen bzw. vergleichbare Zertifizierungen und „Made in Germany“ liegen. Das Innenministerium wird im Rahmen seiner Kompetenz darauf hinwirken, dass der betriebliche Einsatz von Verschlüsselungstechnologien und -produkten in Abhängigkeit von den wirtschaftlichen Sicherheitskosten dem „Stand der Technik“ sowie den Empfehlungen des BSI entsprechen.	
8	Wir unterstützen diese Vorhaben und empfehlen der Landesregierung insbesondere in Anlehnung an die Forderungen der Datenschutzkonferenz - eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen, - die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen, Plattformen zu fördern,	Die Landesregierung teilt mit, dass sie auf den Einsatz von Transportprotokollen und Verfahren setzen wird, die eine möglichst einfache Anwendung von Verschlüsselungstechniken erlauben. In einer gesamtheitlichen Sicht wird bei den laufenden Planungen auch die Kommunikation zu den Bürgern und der Wirtschaft mit betrachtet. Gängige Verschlüsselungstechniken sollen hier unterstützt, durchgehend implementiert und die Nutzung durch flankierende Maßnahmen, wie z. B. dem leichten Zugang zu benötigten Verschlüsselungszertifikaten, erleichtert werden. Ebenso soll bei der Beteiligung an entsprechenden Entwicklungen auf die Umsetzung der genannten Ziele hingewirkt werden.	4.1.10

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 12. TB
	- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und - kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren.		
9	Wir appellieren daher an den Landtag, den Gesetzestext entsprechend den von uns gegebenen Empfehlungen zu ändern.	Die Landesregierung verweist darauf, dass aus ihrer Sicht keine Änderungen notwendig seien.	5.3.1
10	Wir empfehlen dem eGo-MV, die erforderlichen personellen Ressourcen bereitzustellen und geeignete Notfallpläne zu entwickeln, um künftig akute Sicherheitsprobleme unverzüglich bewältigen zu können.	Die Landesregierung weist darauf hin, dass es nach ihrem Informationsstand bislang keinen Sicherheitsvorfall gegeben hat. Ferner verweist die Landesregierung darauf, dass für die Erstellung der Notfallpläne zur unverzüglichen Bewältigung akuter IT-Sicherheitsprobleme die Kommunen selbst zuständig sind. Es ist bisher nicht flächendeckend gelungen, in Ergänzung des landesseitigen zentralen Managementsystems für Informationssicherheit (ISMS) und des BeLVIS auch eine konzentrierend kommunale Instanziierung zu finanzieren, aufzubauen und in Arbeitsbereitschaft zu versetzen. Die Kernfrage einer lückenlosen Finanzierung muss vor der konkreten organisatorischen und technischen Umsetzung des ISMS im kommunalen Raum gelöst werden. Der eGo-MV hat 2015 nach einer Schätzung die kommunalseitigen Kosten mit bis zu ca. 2 Mio. Euro beziffert und eine zwischen Land und Kommunen aufgeteilte Finanzierung vorgeschlagen. Der vorgeschlagene Lösungsansatz wird weiterhin zu erörtern sein.	5.4.3

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 12. TB
11	Wir empfehlen dem Ministerium für Inneres und Sport Mecklenburg-Vorpommern den Abschluss eines Vertrages mit dem eGo-MV zum Betrieb des Sicherungsregisters für das Personenstandswesen nach den Vorschriften zur Datenverarbeitung im Auftrag.	Die Landesregierung weist darauf hin, dass das Innenministerium seit der Errichtung des zentralen Sicherungsregisters, die durch § 1 Abs. 1 S. 3 der Sicherungsregisterverordnung eröffnete Möglichkeit prüfe, den Betrieb des Sicherungsregisters durch eine Körperschaft des öffentlichen Rechts wahrnehmen zu lassen. Derzeit existiere für den Betrieb des Sicherungsregisters des Personenstandswesens ein Vertrag des Landes mit dem technischen Betreiber der DVZ-GmbH in dem auf die Belange des Datenschutzes eingegangen werde. Ein solcher Vertrag wurde seitens des Innenministeriums jedoch bislang nicht zur Prüfung vorgelegt. Es wird darauf hingewiesen, dass das Innenministerium durch die Sicherungsregister-verordnung bisher nicht verpflichtet sei, den Betrieb des Sicherungsregisters an den Zweckverband zu übertragen. Es bestehe lediglich die Möglichkeit der Übertragung. Solange das Innenministerium den Betrieb des Sicherungsregisters nicht übertragen hat, ist es selbst in der Pflicht, die entsprechenden Verträge mit dem technischen Dienstleister DVZ M-V GmbH selbst abzuschließen. Der Verweis des Innenministeriums auf andere zwischen dem Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern, den Standesämtern und der DVZ M-V GmbH abgeschlossenen Verträge geht deshalb fehl.	5.4.4

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 12. TB
12	Wir empfehlen der Landesregierung, wesentliche Grundsätze im Melderecht normenklar im LMG und nicht untergesetzlich zu regeln.	Die Landesregierung verweist darauf, dass die Prüfung der Vorschläge im Rahmen des Gesetzgebungsverfahrens erfolgen wird. Bisher ist noch immer keine Umsetzung erfolgt.	5.4.8
13	Wir empfehlen den Krankenhäusern, ärztlichen und zahnärztlichen Praxen und anderen Partnern der klinischen Krebsregistrierung unseres Landes, diese Entschließung zu beachten.	Die Landesregierung hat keine Bedenken gegen die Empfehlung.	5.6.3
14	Wir empfehlen der Landesregierung, die flächendeckende Verfügbarkeit von Kartenlesern und Signaturkarten für die qualifizierte elektronische Signatur voranzutreiben und gleichzeitig zu prüfen, welche anderen der in § 3a Abs. 2 VwVfg M-V genannten sicheren Verfahren eingesetzt werden können.	Die Landesregierung teilt mit, dass sie den datenschutzgerechten Einsatz elektronischer Identifizierungs- und Signaturverfahren unterstützen wird. Nach unserem Kenntnisstand wird in der Regel aus Kostengründen auf einen Einsatz verzichtet.	5.7.2
15	Wir empfehlen den Verantwortlichen im Bereich Schule, auf die automatisierte Verarbeitung von Daten mit höherem Schutzbedarf mit Hilfe von Verwaltungs- und Lernsoftware zu verzichten, solange dafür keine datenschutzkonforme Software am Markt verfügbar ist. Schon bei der Konzipierung derartiger Softwareprodukte ist in jedem Falle das Gebot der Datensparsamkeit zu berücksichtigen.	Aus Sicht der Landesregierung ist vor dem Hintergrund, dass sich das digitalisierte und internetbasierte Lernen und Lehren rasch ausweiten wird, ein Verzicht auf die automatisierte Verarbeitung von Daten mit höherem Schutzbedarf keine Lösung. In enger Zusammenarbeit aller diesbezüglich relevanten und beteiligten Institutionen des Landes, insbesondere unter Beteiligung des Bildungsministeriums, sollen zeitnah Listen bereits datenschutzrechtlich geprüfter Produkte zusammengestellt und zentral veröffentlicht werden. Bisher ist dem LfDI M-V keine Liste bekannt, in der die Institutionen des Landes, insbesondere unter Beteiligung des Bildungsministeriums, bereits datenschutzrechtlich geprüfte Produkte zusammengestellt und zentral veröffentlicht haben.	5.10.1

2 Vorsitz der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)

2.1 Turnusmäßige Sitzungen

Die Datenschutzbeauftragten des Bundes und der Länder tagen zweimal jährlich unter turnusmäßig wechselndem Vorsitz. Im Jahr 2016 war es unsere Aufgabe, als Vorsitzland die beiden Konferenzen der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) zu organisieren und durchzuführen sowie die Aktivitäten der einzelnen Aufsichtsbehörden im gesamten Jahr 2016 zu koordinieren.
Der Vorsitz war geprägt durch die am 27. April 2016 vom Europäischen Parlament verabschiedete und am 25. Mai 2016 in Kraft getretene Europäische Datenschutz-Grundverordnung (*DS-GVO*), siehe Abschnitt 3.1. Wesentliche Aufgabe des Konferenzvorsitzes war es, die neuen Formen der Zusammenarbeit der deutschen Aufsichtsbehörden untereinander auf den Weg zu bringen und die Anpassung des deutschen Rechts an die DS-GVO zu begleiten. Die Tagesordnungen der Frühjahrskonferenz in Schwerin und der Herbstkonferenz in Kühlungsborn waren daher von europäischen Themen geprägt. Beraten wurde sowohl über die Auswirkungen der DS-GVO auf die künftigen, möglichst einheitlichen Datenschutzstandards in Deutschland als auch auf technische und organisatorische Details der Zusammenarbeit, siehe Punkt 3.1.2, der deutschen Aufsichtsbehörden untereinander und mit den Aufsichtsbehörden der anderen Mitgliedsstaaten. In diesem Zusammenhang hat die Konferenz in einer Entschließung ihre Auffassung verdeutlicht, dass eine Stärkung des Datenschutzes in Europa nur dann gelingen wird, wenn bei der Anpassung des nationalen Rechts an die DS-GVO die nationalen Spielräume genutzt werden[1]. Neben den Absprachen der Aufsichtsbehörden untereinander waren aber auch Gespräche mit Vertretern der Wirtschaft zu organisieren, um deren Stand der Umsetzung der DS-GVO zu erörtern und gegebenenfalls zu beeinflussen.

Die intensive Auseinandersetzung mit der DS-GVO hat auch verdeutlicht, welche neuen Aufgaben auf alle Mitglieder der Datenschutzkonferenz in ihrer Eigenschaft als Aufsichtsbehörde zukommen und welche zusätzlichen personellen und finanziellen Ressourcen erforderlich sein werden, siehe auch Punkt 3.1.2. Die Datenschutzkonferenz hat in einer weiteren Entschließung an die Gesetzgeber in Bund und Ländern appelliert, rechtzeitig die haushaltsrechtlichen Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen[2].

Besonders schwierig gestaltete sich der Konferenzvorsitz, wenn es zwischen den Mitgliedern der Konferenz unterschiedliche Auffassungen gab. Dies liegt aber in der Natur der Sache, denn die Datenschutzbeauftragten von Bund und Ländern sind völlig unabhängig und unterschiedliche Auffassungen in der Sache sind daher völlig legitim. Deutlich wurden solche Unterschiede etwa in der Frage der Besetzung des Europäischen Datenschutzausschusses. Für ein föderales System wie Deutschland bringt sie besondere Herausforderungen mit sich, da jeder Mitgliedsstaat im Ausschuss nur über eine Stimme verfügt. Strittig war in der Konferenz beispielsweise die Verteilung der Stimmrechte zwischen Bund und Ländern.

[1] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Entschl_DS_staerken.pdf
[2] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Ent_Ressourcen.pdf

In der sogenannten Kühlungsborner Erklärung [3] haben sich daher auch nur die Datenschutzbehörden der Länder zu Wort gemeldet und den Bundesgesetzgeber aufgefordert, bei der gesetzlichen Regelung des Vertreters der deutschen Aufsichtsbehörden im Ausschuss der Unabhängigkeit aller Aufsichtsbehörden und der Zuständigkeitsverteilung zwischen Bund und Ländern Rechnung zu tragen.

Neben den durch die DS-GVO bestimmten Themen hat die Konferenz natürlich auch über Datenschutzfragen im nationalen Kontext beraten. In der Frühjahrssitzung in Schwerin wurden etwa die Datenschutzrisiken von Wearables und Gesundheits-Apps erörtert und eine Entschließung hierzu verabschiedet[4]. Im Zusammenhang mit verschiedenen Vorhaben des IT-Planungsrates zum Portalverbund und zu Servicekonten, siehe dazu auch Punkt 7.2, hat die Konferenz in einer Entschließung auf die erforderlichen datenschutzrechtlichen Rahmenbedingungen hingewiesen[5]. In der Herbstkonferenz in Kühlungsborn wurde Bilanz gezogen über die gemeinsame Prüfung der Falldatei Rauschgift. In ihrer Entschließung hierzu weist die Konferenz auf gravierende Mängel in der Datei hin und fordert Konsequenzen für die polizeiliche Datenverarbeitung [6] . Auch das sogenannte Videoüberwachungs-Verbesserungsgesetz wurde in der Herbstkonferenz erörtert. Die Mitglieder kritisierten das Vorhaben des Bundesministeriums des Innern (*BMI*), durch dieses Gesetz die Rahmenbedingungen für Videoüberwachungen zu verändern, und forderten in einer Entschließung den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen[7].

Insbesondere die Fülle der koordinierenden Aufgaben im Kontext der Datenschutz-Grundverordnung erforderte neben den beiden turnusmäßigen Konferenzen fünf außerplanmäßige Sonderkonferenzen. Um diese Konferenzen als Tagesveranstaltung für alle Mitglieder durchführen zu können, tagten wir in Berlin und konnten dabei in den meisten Fällen auf den hervorragenden Veranstaltungsdienst der Vertretung des Landes Mecklenburg-Vorpommern beim Bund in Berlin zurückgreifen. Dennoch hat der Konferenzvorsitz eine kleine Aufsichtsbehörde wie die Mecklenburg-Vorpommerns zeitlich und personell bis an die Grenzen belastet. Insbesondere dem Engagement aller Mitarbeiterinnen und Mitarbeiter der Dienststelle ist es zu verdanken, dass diese anspruchsvolle Aufgabe zur Zufriedenheit aller Konferenzmitglieder gemeistert werden konnte.

[3] https://www.datenschutz-mv.de/static/DS/Dateien/Themen/Kuehlungsborner_Erklaerung.pdf
[4] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Entschl_Wearables.pdf
[5] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Entschl_Servicekonten.pdf
[6] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Entsch_Falldatei_Rauschgift.pdf
[7] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Entsch_Video.pdf

2.2 Zusammenarbeit mit BMI und IMK

Der Konferenzvorsitz im Jahr 2016, siehe Punkt 2.1, war verbunden mit der Begleitung der Anpassung des deutschen Datenschutzrechts an die Europäische Datenschutz-Grundverordnung (*DS-GVO*). Der Schwerpunkt auf Bundesebene lag bei der dafür erforderlichen Novellierung des Bundesdatenschutzgesetzes (*BDSG*).

Um die langjährigen Erfahrungen der Datenschutzaufsichtsbehörden in den Prozess der Novellierung einzubringen, haben wir als Konferenzvorsitz angeboten, die hierfür erforderlichen Gespräche zwischen den Aufsichtsbehörden einerseits und dem für die BDSG-Novelle zuständigen Bundesministerium des Inneren (*BMI*) und der Innenministerkonferenz (*IMK*) andererseits zu organisieren und zu moderieren. Zu diesem Zweck haben wir eine sogenannte Kontaktgruppe ins Leben gerufen, in der die Bundesdatenschutzbeauftragte und einige Landesdatenschutzbeauftragte mit dem Mandat der Datenschutzkonferenz die erforderlichen Abstimmungsgespräche mit den Vertretern des BMI und der IMK führen.

Diese Kontaktgruppe hat unter unserem Vorsitz viermal im Laufe des Jahres 2016 getagt. Es hat sich gezeigt, dass dieses unkonventionelle Format der Zusammenarbeit sehr gut geeignet war, um in konstruktiven Gesprächen die Novelle des BDSG voranzutreiben. Der Bundesgesetzgeber hat von den Erfahrungen der Aufsichtsbehörden profitiert und wir hatten die Möglichkeit, auf die Formulierungen des neuen BDSG Einfluss zu nehmen. Natürlich wurden längst nicht alle Hinweise und Formulierungsvorschläge der Datenschutzbeauftragten berücksichtigt, in vielen Bereichen konnten jedoch sinnvolle Kompromisse gefunden werden.

Dass sich das Konzept der Kontaktgruppengespräche bewährt hat, verdeutlicht auch die Tatsache, dass die Vertreter der IMK gegenüber dem Konferenzvorsitz des Jahres 2017 ihr Interesse bekundet haben, die Arbeiten der Kontaktgruppe fortzuführen, um die zweite Stufe der Anpassung des Datenschutzrechts des Bundes an die Datenschutz-Grundverordnung gemeinsam zu erörtern.

2.3 Der 11. Europäischer Datenschutztag

Alljährlich am 28. Januar wird der Europäische Datenschutztag begangen. Die zentrale Veranstaltung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder richtet traditionsgemäß der turnusmäßige Vorsitzende der Konferenz des Vorjahres aus. Somit war es unsere Aufgabe, die Veranstaltung im Januar 2017 zum 11. Europäischen Datenschutztag zu organisieren.

Als Thema der Veranstaltung, die am 30. Januar 2017 im Abgeordnetenhaus von Berlin stattfand, hatten wir den Titel „Diktatur der Daten? - Privatsphäre und Selbstbestimmung im Zeitalter von Big Data und Algorithmen “ gewählt. Mit diesem Thema wollten wir eine Verbindung herstellen zwischen der Europäischen Datenschutz-Grundverordnung (*DS-GVO*), die am 25. Mai 2016 in Kraft getreten ist, und der rasanten Entwicklung der Technik. Die DS-GVO legt fest, dass niemand sich einer Entscheidung unterwerfen muss, die ausschließlich auf einer automatisierten Verarbeitung beruht.

Die technischen Entwicklungen im Bereich von Big Data, künstlicher Intelligenz und Algorithmen werfen jedoch die Frage auf, ob diese Bestimmung in der Praxis umsetzbar sein wird. Schon heute treffen Algorithmen Entscheidungen, die vom Menschen kaum noch beeinflussbar sind, etwa wenn es um die schnelle Analyse großer Datenmengen oder die Vorhersage des Verhaltens von Menschen geht. Mit der Veranstaltung sollte der Versuch gemacht werden, die Frage zu klären, ob wir diese Algorithmen noch beherrschen oder ob uns die Automatisierung der Gesellschaft durch Big Data und Algorithmen droht.

Als Hauptredner hatten wir *Yvonne Hofstetter*, Geschäftsführerin der Teramark Technologies GmbH, gebeten, zum Thema „Umgebungsintelligenz im Internet der Dinge: Das Ende der Privatsphäre?“, und *Professor Dr. Harald Welzer*, Honorarprofessor für Transformationsdesign an der Europa-Universität Flensburg, zum Thema „Die smarte Diktatur. Warum die Digitalisierung antimodern ist.“ zu referieren. Die als Big-Data- und Silicon-Valley-Kritiker bekannten und Talkshow-erfahrenen Vortragenden waren sich einig, dass die Digitalisierung das Risiko in sich berge, die Privatheit und andere Grundvoraussetzungen moderner Demokratien sukzessive abzuschaffen und dass neue Diktaturen entstehen könnten.

Professor Dr. Welzer machte eine eigentümliche Verschiebung im grundsätzlichen Machtverhältnis aus. Noch immer glaubten die Menschen, dass keiner mehr über sie weiß als sie selbst. Dies sei die Basis für die demokratische Verfassung, für autonom handelnde Subjekte. Heute sei aber davon auszugehen, dass es immer irgendetwas gibt, eine Organisation, einen Algorithmus, eine Matrix, die mehr weiß. Überwachung bezeichnete *Professor Dr. Welzer* als die höchste reale Gefahr, die unsere Gesellschaftsform unterminiert. Das Smartphone spiele dabei eine entscheidende Rolle, denn es gebe kaum eine andere Technik, die so fundamental in die menschlichen Verhaltensweisen eingreife.

Yvonne Hofstetter wies insbesondere auf die Risiken sozialer Netzwerke hin. Was dort zu lesen sei, habe viel mit Übertreibungen bis hin zur dreisten Lüge zu tun. Es gehe darum, eine Meinung und Überzeugung zu schaffen. *Yvonne Hofstetter* kritisierte zudem Profiling bis hin zum geplanten „People Score“ in China, Diskriminierung durch Algorithmen und „technologischen Rassismus“. Lernende Systeme könnten in eng umrissenen Gebieten zwar außergewöhnlich gute Entscheidungen treffen. Generell seien Künstliche Intelligenzen aber nichts als Optimierungsverfahren, hinter denen nicht viel stecke.

In der anschließenden Podiumsdiskussion griff *Professor Dr. Gerd Gigerenzer*, Direktor am Max-Planck-Institut für Bildungsforschung, diese These auf. Mit wenigen Ausnahmen seien Algorithmen nicht so gut, wie vermutet wird, betonte er. Ein großer Teil von Big Data drehe sich um eine Art Absicherungskultur und psychologisches Spiel, während gar nicht getestet werde, was dort tatsächlich möglich sei. So hätten Tests ergeben, dass einfache heuristische Verfahren besser seien als Software für das sogenannte Predictive-Policing.

Als weiterer Teilnehmer der Podiumsdiskussion wies *Dr. Thilo Weichert* vom Netzwerk Datenschutzexpertise darauf hin, dass Politiker Big Data wohl deshalb favorisieren, weil es ihre Entscheidungen rationalisieren soll. Er vermute, dass Bundeskanzlerin Angela Merkel und einige ihrer Kabinettskollegen nur noch vom Datenreichtum schwärmten, weil sie hoffen, „etwas vom großen Kuchen aus dem Silicon Valley abzukriegen".

Jan Phillip Albrecht, Mitglied des Europäischen Parlaments und „Vater" der Europäischen Datenschutz-Grundverordnung (DS-GVO), äußerte in der Podiumsdiskussion seine tiefe Überzeugung, dass diese Regelungen durchaus geeignet wären, die notwendigen Leitplanken für Big Data und Algorithmen zu liefern.

In der Rückschau auf den Europäischen Datenschutztag 2017 können wir feststellen, ein höchst aktuelles Thema aufgegriffen zu haben und vielleicht sogar den Anstoß für eine große Zahl weiterer Veranstaltungen zu diesem Thema gegeben zu haben. Auch die Datenschutzkonferenz hat sich zu diesem Thema geäußert und in ihren „Grundsatzpositionen und Forderungen für die neue Legislaturperiode"[8] gefordert, für den Einsatz von Algorithmen im Hinblick auf Transparenz, Kontrolle und Begrenzung klare gesetzliche Regelungen zu schaffen, siehe dazu auch Punkt 5.1.6.

3 Neuer Europäischer Rechtsrahmen im Datenschutz

3.1 Neues EU-Recht im Datenschutz - die europäische Datenschutz-Grundverordnung (DS-GVO)

Die EU-Verordnung 2016/79 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DS-GVO)" wurde im Amtsblatt der EU am 4. Mai 2016 veröffentlicht. Am 25. Mai 2016 trat sie in Kraft und wird ab dem 25. Mai 2018 Wirksamkeit entfalten (siehe Art. 99 DS-GVO). Mit Wirksamkeit der DS-GVO wird die bisherige Datenschutz-Richtlinie 95/45/EG aufgehoben.

Damit besteht in der Zeit zwischen dem 4. Mai 2016 und dem 25. Mai 2018 ein rechtlicher Übergangszeitraum, der die notwendige Anpassung an das neue EU-Recht ermöglichen soll.

Neben diesem gestuften Inkrafttreten ist zu beachten, dass die DS-GVO ihre Schutzwirkung innerhalb der EU nicht abschließend entfalten will und kann. Als „GRUNDverordnung" sieht sie zwar allgemeine und grundsätzliche Regeln zur Verarbeitung personenbezogener Daten vor, sie enthält aber auch eine Vielzahl von Klauseln (sog. Öffnungsklauseln), die den Mitgliedstaaten ermöglichen, ergänzende und konkretisierende Vorschriften entweder weiterhin zu verwenden oder neu zu schaffen. Dabei ist der häufig verwendete Begriff „Öffnungsklauseln" irreführend, da es sich vielmehr um „Spezifizierungsklauseln" handelt. Dem entsprechenden Mitgliedstaat ist es nur gestattet, in dem durch die Verordnung vorgegebenen Rahmen konkretisierend bzw. spezifizierend zu regeln.

[8] https://www.datenschutz-mv.de/serviceassistent/_php/download.php?datei_id=1593517

Der Deutsche Bundestag versuchte dies, indem er bisher das Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) am 28. April 2017 beschloss, ein entsprechender (notwendiger) Beschluss des Bundesrates erfolgte am 12. Mai des gleichen Jahres. Ein wesentlicher Teil dieses Paketes ist das neugefasste BDSG (BDSGnF).

In welchem Umfang dieses BDSGnF neben der DS-GVO europarechtlich Bestand haben wird, bleibt hingegen abzuwarten. So wurde das Gesetzgebungsverfahren von massiver Kritik begleitet, da es nach Auffassung zahlreicher Kritiker weitgehend dem überdehnten Verständnis der „Öffnungsklauseln“ entspräche (s. o.) und zudem an mehreren Stellen gegen das explizite Wiederholungsverbot der DS-GVO verstoße. Grundsätzlich gilt jedenfalls, dass jede bestehende nationale Datenschutzvorschrift vor dem Hintergrund der DS-GVO als höherrangigem Recht europarechtsfreundlich auszulegen ist.

Letzteres gilt auch für das zwischenzeitlich als Anpassungsrecht in Angriff genommene Landesdatenschutzrecht in unserem Bundesland:

So wurde schon im Rahmen einer Kleinen Anfrage im August 2017 (Drucksache 7/818) seitens der Landesregierung festgehalten, dass seinerzeit 46 Landesgesetze und acht Verordnungen als Anpassungsbedarf identifiziert wurden. Zum Zeitpunkt der Erstellung dieses Berichtes wurde seitens der Landesregierung im Rahmen der Drucksache 7/1568(neu) auch der Entwurf eines Gesetzes zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften im Zuständigkeitsbereich des Ministeriums für Inneres und Europa an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 ins parlamentarische Verfahren übergeben.

Auch dieser Entwurf wurde seitens unserer Behörde kritisch begleitet und an manchen dortigen Regelungen hegen wir sehr ernste Zweifel in Bezug auf deren europarechtliche Konformität. Hierzu werde ich mich im Rahmen der entsprechenden Anhörungen konkret äußern.

Unabhängig von den - hier nur kurz skizzierten und durch die EU noch zu prüfenden - nationalstaatlichen Datenschutz-Regelungen bringt die DS-GVO bereits vor ihrer Wirksamkeit einen erheblichen Anpassungsbedarf mit sich.

Die für die Verarbeitung von personenbezogenen Daten Verantwortlichen haben ihre Verfahren spätestens ab Wirksamkeit der Verordnung so zu gestalten, dass eine möglichst hohe Datenschutzfreundlichkeit gewährleistet ist (Art. 25 DS-GVO). Zudem werden dem Betroffenen signifikant ausgeprägtere Löschungs- und Berichtigungsansprüche gewährt (Art. 17 DS-GVO) - dies ergänzt durch einen expliziten Anspruch auf Datenportabilität (Art. 20 DS-GVO).

Die für die Verarbeitung verantwortlichen Unternehmen (und auch Behörden) haben ihrerseits Instrumente und Verfahren zu entwickeln, die in bestimmten Konstellationen eine umfangreiche, qualifizierte, abrechenbare und obligatorische Datenschutzfolgenabschätzung erlauben.

Letztlich leitet die DS-GVO einen Paradigmenwechsel ein. Die für die Datenverarbeitung Verantwortlichen müssen künftig jederzeit nachweisen können, dass sie alle Vorschriften der DS-GVO (und ihrer nationalen Konkretisierungsnormen) einhalten. Infolgedessen entfällt für die Aufsichtsbehörden - soweit dieser Nachweis durch die Verantwortlichen nicht zweifelsfrei erbracht werden kann - die Verschuldensermittlung. Im Rahmen dieser Nachweisverpflichtung und Abrechenbarkeit kommt es nunmehr also zu der Verpflichtung der Verantwortlichen, ihre umfangreichen rechtlichen Konformitätsanstrengungen nachvollziehbar, integer und jederzeit verfügbar zu dokumentieren und diese bei Bedarf vorweisen zu können.

Die bei substantiellen Verstößen gegen das Datenschutzrecht drohenden (erhöhten) Bußgelder von bis zu 20 Mio. Euro oder - sofern höher - bis zu 4 % des weltweiten Jahresumsatzes erreichen neue Dimensionen und sorgen (auch vor dem Hintergrund der etwas übertrieben anmutenden entsprechenden öffentlichen Diskussion) dafür, dass die Einhaltung des Datenschutzes stärker in den Fokus der strategischen Entscheidungen und letztlich auch der Compliance rückt.

Herstellern, die mit der DS-GVO konforme Produkte anbieten und die Konformität ihren Kunden gegenüber nachweisen können, eröffnen sich zusätzliche Marktchancen - diese sollten breit genutzt werden.

Hinsichtlich der schon in unserem zwölften Tätigkeitsbericht, Einleitung, dargestellten Folgen der DS-GVO für unsere Behörde, bleibt auf die folgenden wesentlichen Punkte hinzuweisen:

Mit der zwischenzeitlichen Entsperrung von fünf befristeten Personalstellen wurde ein erster dringend notwendiger struktureller Schritt zur Konsolidierung einer bisher stets unterbesetzten Aufsichtsbehörde getan. Der Landtag hat hiermit konkludent einen entsprechenden Ausstattungsbedarf unstreitig gestellt. Selbstverständlich ist mit dieser ersten „Notmaßnahme“ die erforderliche Umstrukturierung und erforderliche personelle Anpassung unserer Behörde an die Vielzahl zusätzlicher Aufgaben noch nicht abgeschlossen.

In einem nächsten Schritt wurde vor dem Hintergrund streitiger Anpassungsbedarfe der Landesrechnungshof gebeten, in unserer Behörde eine eingehende Organisationsprüfung unter anderem mit dem Ziel der objektiven Feststellung des personellen Ausstattungsbedarfes durchzuführen. Diese Prüfung begann im Spätsommer 2017 und ist zum Zeitpunkt der Fertigung dieses Berichtes noch nicht ganz abgeschlossen.

Zusätzlich hat sich unsere Behörde - auch unter Würdigung der Anregungen des Landesrechnungshofes - organisatorisch auf die zu erwartenden praktischen Neuerungen der DS-GVO umstrukturiert, eine aufwendige Maßnahme, die unter anderem in einem neuen Organigramm ihren Ausdruck fand. Dieses neue und noch zwangsläufig unfertige Organigramm setzt nach wie vor einen angemessenen und auf eingehenden Aufgabenanalysen fundierenden Stellenzuwachs von derzeit 9 Personalstellen voraus. Die weiteren Verhandlungen hierzu werden demnach widerspiegeln, welchen Stellenwert die DS-GVO und damit die Grundrechte der Artikel 1 und 2 unseres Grundgesetzes (GG) in unserem Bundesland einnehmen.

3.1.1 Ausstattung der Dienststelle

Umzug der Dienststelle

Die von uns seit 1998 genutzte Dienststelle genügte seit einigen Jahren nicht mehr den Anforderungen hinsichtlich der erforderlichen Bürofläche und der technischen Ausstattung. Nach mehreren vergeblichen Anläufen in den vergangenen Jahren konnten wir Anfang 2016 mit konkreten Planungen für eine neue Dienststelle beginnen. Bei der Ausgestaltung der Anforderungen an einen sicheren Betrieb der Rechentechnik im Serverraum und einer ausreichenden Verkabelung der Büro- und Beratungsräume haben wir uns sehr weitgehend an den Vorgaben aus dem Konzept zum Betrieb der Kommunikationsinfrastruktur für die Landesverwaltung (KommSt 2017) orientiert, wenngleich diese erst ab dem Jahr 2017 verbindlich gelten sollten. Darüber hinaus mussten sicherheitstechnische Vorgaben berücksichtigt werden, die aus dem Bereich des Geheimschutzes resultieren. Der eigentliche Umzug wurde dann so geplant und realisiert, dass die Dienststelle nur wenige Tage eingeschränkt arbeitsfähig war. Die neue Dienststelle bietet nun ausreichend Kapazität, um allen Mitarbeiterinnen und Mitarbeitern angemessene Arbeitsbedingungen bieten zu können. Wir gehen davon aus, dass wir auch den wachsenden Anforderungen, die sich aus der Europäischen Datenschutz-Grundverordnung (*DS-GVO*) ergeben, gerecht werden können.

Inbetriebnahme einer Videokonferenzanlage

Schon in der Vergangenheit waren wir rechtlich verpflichtet, mit anderen Datenschutzbehörden eng zusammenzuarbeiten, sowohl auf nationaler Ebene als auch über die Grenzen Deutschlands hinweg. Die Forderung nach einheitlicher Anwendung der DS-GVO (Art. 51 Abs. 2) wird einerseits zu einer noch intensiveren Mitarbeit in verschiedenen nationalen und internationalen Gremien führen, andererseits aber auch die Zusammenarbeit der deutschen Datenschutzbehörden verstärken, etwa im Rahmen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, siehe Punkt 2, und der zahlreichen Gremien der Konferenz, etwa der Arbeitskreise.

Würden die organisatorischen Rahmenbedingungen unverändert beibehalten werden, würden diese Verpflichtungen zwangsläufig zu mehr Zeitaufwänden, zu erhöhter Reisetätigkeit und zu steigenden Reisekosten führen. Um einerseits die Produktivität und Effizienz der Zusammenarbeit über mehrere Ebenen hinweg zu steigern und andererseits die Kosten und Zeitaufwände zu senken, haben wir uns entschlossen, eine Videokonferenzanlage anzuschaffen. Derartige Anlagen stellen zwar keinen gleichwertigen Ersatz von gemeinsamen Beratungen vor Ort dar, bieten aber gegenüber Telefonkonferenzlösungen erhebliche Vorteile, da sie eine ähnliche Gesprächsatmosphäre wie die persönlichen Treffen vermitteln. Zudem ermöglicht eine Videokonferenzlösung das Präsentieren von Inhalten und ein gleichzeitiges Bearbeiten von Dokumenten, wodurch ein konzentriertes und zielgerichtetes Arbeiten möglich wird. Um den hohen Anforderungen an die Sicherheit der Verbindung gerecht zu werden, ermöglicht die von uns verwendete Videokonferenzlösung eine Ende-zu-Ende-Verschlüsselung der gesamten Kommunikation. Inzwischen ist die verfügbare Technik auch so nutzerfreundlich und ergonomisch ausgereift, dass selbst mehrstündige Videokonferenzen problemlos realisierbar sind.

Dass bereits eine breite Akzeptanz von Videokonferenztechniken bei Bund und Ländern vorhanden ist, zeigt der Blick auf den IT-Planungsrat (*IT-PLR)*, siehe Punkt 7. Inzwischen

finden zahlreiche Besprechungen verschiedener Gremien des IT-PLR als Videokonferenzen statt. Auch an den Vorbesprechungen auf der Ebene der Abteilungsleiter nehmen wir inzwischen regelmäßig über Videokonferenzen teil.

Umbau der IT-Infrastruktur

Angesichts der nach wie vor unzureichenden Personalausstattung sind wir ständig auf der Suche nach Einsparpotentialen. Um den Aufwand bei der Administration unserer IT-Infrastruktur senken und die stetig zunehmende Komplexität von Hard- und Software dennoch beherrschen zu können, haben wir uns entschieden, unsere IT-Infrastruktur an die neuen Anforderungen anzupassen. Nachdem wir schon in den letzten Jahren Virtualisierungstechniken im Bereich der Server und zentralen Anwendungen der Dienststelle eingesetzt haben, war folgerichtig der nächste Schritt fällig: der Einsatz einer Virtual Desktop Infrastructure (*VDI*). Im Laufe des Jahres 2017 haben wir einen virtuellen Terminalserver aufgesetzt und die ersten Arbeitsplatzcomputer durch einfach zu administrierende Thin-Clients ersetzt. Auf diese Weise kann auch weiterhin jede Nutzerin und jeder Nutzer auf die gewohnte Arbeitsumgebung zurückgreifen. Da die virtualisierten Clients sehr gut zentral verwaltet werden können, können wir künftig schnell und flexibel die einzelnen Arbeitsplätze konfigurieren. Im Laufe des Jahres 2018 wird die gesamte Dienststelle die neue Umgebung nutzen können.

Neugestaltung der Webseite

Die Webseite des Landesbeauftragten ist ein wichtiges Informations- und Kontaktangebot für die öffentliche Verwaltung, für Unternehmen und nicht zuletzt auch für die Bürgerinnen und Bürger des Landes. Sie informiert über Ergebnisse von Konferenzen und Arbeitskreisen der unabhängigen Aufsichtsbehörden des Bundes und der Länder, gibt praktische Hinweise und Umsetzungshilfen in Form von Orientierungshilfen, Musterpapieren und Beispielen und bietet verschiedene Möglichkeiten der Kontaktaufnahme mit uns und der Abgabe gesetzlich vorgeschriebener Meldungen bei uns als Aufsichtsbehörde. Nicht zuletzt soll die Seite aber auch über die vielfältige Arbeit unserer Behörde informieren, beispielsweise in Form von regelmäßigen Pressemitteilungen, Projektarbeiten, Tätigkeitsberichten und Veranstaltungshinweisen.

Neben den Anforderungen an Aktualität der Inhalte müssen auch immer die technologischen Anforderungen der Geräte berücksichtigt werden, mit denen auf die Inhalte zugegriffen wird. Dies erfordert eine kontinuierliche Weiterentwicklung der technischen Basis der Webseite. Da in den vergangenen Jahren die Seitenzugriffe über mobile Endgeräte wie Tablets oder Smartphones konstant zugenommen haben, ist eine Ausrichtung des Webseitendesigns auf die neuen kleineren Displaygrößen unabdingbar gewesen.

Hierzu haben wir im August des Jahres 2017 die Webseite komplett neu gestaltet. Nutzerinnen und Nutzer erkennen die Neugestaltung an einem neuen Design mit einer neuen Farbgestaltung und einer optimierten Menüausrichtung sowie einer neuen Suchmaschine. Von außen nicht zu erkennen sind grundlegende Änderungen im Hintergrund. Gleichzeitig mit dem Wechsel des Designs erfolgte auch der Wechsel der administrativen Plattform. Für die Pflege der Inhalte nutzen wir nun ein sogenanntes Content-Management-System (*CMS*) und stützen uns dabei auf eine Basiskomponente der E-Government-Infrastruktur des Landes. Das neue CMS ermöglicht uns nun ein erleichtertes und effizientes Einpflegen von neuen Inhalten und führt somit zur Einsparung von zeitlichen und personellen Ressourcen unserer Dienststelle. Besucherinnen und Besucher haben den zusätzlichen Vorteil, nun nicht nur den Webseiteninhalt, sondern auch die Inhalte von hinterlegten Dokumenten durchsuchen zu können. Zudem passt sich die Webseitendarstellung nun auch automatisch an die unterschiedlichen Displaygrößen an, sodass ein Navigieren durch die Webseite sowohl mit dem klassischen Personalcomputer als auch mit dem Tablet oder Smartphone leicht von der Hand geht.

Personal

Auf die neuen Anforderungen, die die DS-GVO an die Ausstattung der Aufsichtsbehörden stellt, sind wir schon mehrfach in diesem Bericht eingegangen. Die DS-GVO fordert in Artikel 53 Abs. 3 jeden Mitgliedsstaat auf, die Aufsichtsbehörden mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen auszustatten, die sie benötigen, um ihre Befugnisse effektiv wahrnehmen zu können. Während im Bereich der räumlichen und technischen Ausstattung durch den Umzug in die neue Dienststelle bereits die ersten Schritte in die richtige Richtung gemacht wurden, bleibt bei der personellen und finanziellen Ausstattung unserer Behörde noch erheblicher Nachholbedarf.

Um die durch die DS-GVO gestiegenen personellen Anforderungen möglichst genau beziffern zu können, haben wir die Datenschutz-Grundverordnung hinsichtlich der neuen Aufgaben detailliert analysiert. Wir haben festgestellt, dass bei uns als Aufsichtsbehörde etwa 55 neue Aufgaben anfallen. Zum größten Teil handelt es sich dabei um völlig neue Aufgaben innerhalb eines starren und gerichtsbewehrten Fristenkorsetts. Diese Aufgaben erfordern oftmals einen hohen europaweiten Abstimmungsbedarf, der auch fremdsprachlich zu erfolgen hat. Unsere Analyse hat gezeigt, dass mit dem bisher zur Verfügung stehenden Personal von 22 Beschäftigten, von denen 5 Beschäftigte nur befristet angestellt sind, diese Aufgaben nicht zu bewältigen sind. Folgerichtig haben wir im Rahmen der Verhandlungen zum Doppelhaushalt 2018/2019 einerseits die Entfristung der 5 oben genannten Stellen beantragt und darüber hinaus 9 neue Stellen gefordert.

In seiner ersten Befassung mit unseren Stellenanträgen war es dem Finanzausschuss des Landtages MV noch nicht möglich, eine Entscheidung zu treffen. Im Juni 2017 richtete er eine Prüfbitte an den Landesrechnungshof MV. Dieser sollte einerseits eine Organisationsuntersuchung in unserer Dienststelle für das Jahr 2016 durchführen, um den Aufgabenbestand und die Stellenausstattung bewerten zu können, und eventuell vorhandene Kapazitätsreserven beziffern. Darüber hinaus sollte er die aus der DS-GVO resultierenden Mehrbedarfe bewerten.

In einem ersten Zwischenbericht stellte der Landesrechnungshof nach Auswertung der Organisationsuntersuchung fest, dass alle Beschäftigten zwischen 100 % und 105 % ausgelastet sind. Auf die gesamte Dienststelle bezogen lag die Auslastung bei 21,359 Vollzeitäquivalenten (*VZÄ*) bei einem verfügbaren Personal von 20.975 VZÄ. Folgerichtig hat der Landesrechnungshof dem Finanzausschuss empfohlen, die Befristung der 5 Stellen aufzuheben. Der Finanzausschuss folgte dieser Empfehlung und beschloss Ende 2017 die Schaffung von 5 neuen Stellen mit Wirkung vom 1. Januar 2018.

Der zweite Teil der Prüfung des Landesrechnungshofes, die Bewertung der von uns beschriebenen personellen Mehrbedarfe, war zum Ende des Berichtszeitraumes noch nicht abgeschlossen. Um dem Landtag auch nach Verabschiedung des Doppelhaushaltes 2018/2019 Handlungsoptionen einzuräumen, wurden die von uns beantragten Stellen zwar in den Stellenplan unserer Behörde aufgenommen, aber mit einem Sperrvermerk versehen. Es bleibt abzuwarten, ob der Landesrechnungshof die von uns formulierten Mehrbedarfe mitträgt und welche Schlussfolgerungen das Parlament aus den Empfehlungen des Landesrechnungshofes ziehen wird.

Neben einer ausreichenden personellen Ausstattung der Aufsichtsbehörden fordert die DS-GVO auch eine angemessene finanzielle Ausstattung. Art. 52 Abs. 6 DS-GVO konkretisiert diese Forderungen. Die Mitgliedsstaaten müssen sicherstellen, dass die Aufsichtsbehörden zwar der Finanzkontrolle unterliegen, die aber nicht die Unabhängigkeit beeinträchtigt. Zu diesem Zweck sollen Aufsichtsbehörden über eigene, öffentliche, jährliche Haushaltspläne verfügen, die aber Teile des Staatshaushalts sein können. Bereits in seinem ersten Zwischenbericht hat der Landesrechnungshof daher gefordert, für unsere Behörde einen eigenen Einzelplan einzurichten. Er hat darauf hingewiesen, dass es mit der DS-GVO nicht vereinbar ist, unser Budget als Teil des Einzelplans 01 (Kapitel 0102) auszuweisen. Im Entwurf des neuen Landesdatenschutzgesetzes [Drucksache 7/1568(neu)] ist die Landesregierung dieser Empfehlung bisher nicht gefolgt. Nach wie vor sollen die notwendigen Personal- und Sachmittel, die unserer Behörde für die Erfüllung unserer Aufgaben zur Verfügung zu stellen sind, im Einzelplan des Landtages in einem gesonderten Kapitel ausgewiesen werden. Es bleibt abzuwarten, ob im Laufe der parlamentarischen Behandlung des Gesetzentwurfes diese europarechtswidrige Regelung noch korrigiert wird.

3.2 Die JI-Richtlinie

Im Paket mit der Datenschutz-Grundverordnung hat die EU im Jahr 2016 auch die Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI (JI-Richtlinie) verabschiedet. Sie muss bis zum 6. Mai 2018 in nationales Recht umgesetzt werden.

Für die Bereiche, die der Datenschutz-Grundverordnung unterfallen, gilt diese ab Mai 2018 als unmittelbar anwendbares Recht. Landesrecht kommt nur zur Anwendung, wo die Regelungen der Datenschutz-Grundverordnung durch nationales Recht konkretisiert werden dürfen. Die JI-Richtlinie muss hingegen vollständig in Landesrecht umgesetzt werden, denn EU-Richtlinien sind nicht unmittelbar anwendbar.

Der Bundesgesetzgeber hat die Umsetzung der JI-Richtlinie dadurch gelöst, dass er im allgemein geltenden Bundesdatenschutzgesetz vier Teile vorgesehen hat: Ein Teil enthält Durchführungsbestimmungen für die Datenschutz-Grundverordnung, ein Teil enthält Regelungern zur Umsetzung der JI-Richtlinie, ein Teil enthält Regelungen für Bereiche, die weder der Datenschutz-Grundverordnung noch der JI-Richtlinie unterfallen, und ein vorangestellter Teil enthält gemeinsame Regelungen für alle drei Bereiche. Durch dieses Regelwerk wird sichergestellt, dass zum einen keine Regelungslücken entstehen und zum anderen für alle Bereiche ein einheitliches Datenschutzniveau gilt.

Im neu gefassten Landesdatenschutzgesetz ist zur Umsetzung der JI-Richtlinie vorgesehen, dass die Regelungen der Datenschutz-Grundverordnung und des Landesdatenschutzgesetztes entsprechend gelten, soweit gesetzlich nicht etwas anders bestimmt ist.

Um die JI-Richtlinie vollständig umzusetzen, wird diese allgemeine Regelung allerdings nicht ausreichen. Diese wird, wie dies auch jetzt der Fall ist, durch bereichsspezifische konkrete Regelungen ergänzt werden müssen. Dies betrifft vor allem den Abschnitt 3 im Sicherheits- und Ordnungsgesetz für das Land Mecklenburg-Vorpommern. Hier sind einige Anpassungen an das neue EU-Recht vorzunehmen.

3.3 Lehr-Schulungs-und Informationsveranstaltungen zum Europäischen Datenschutzrecht

Unsere Behörde ist auch mit Geltung der kommenden Europäischen Datenschutz-Grundverordnung (*DS-GVO*) eine Aufsichtsbehörde mit Kontroll- und Sanktionsbefugnissen.

Gleichwohl setzen wir primär auf den bewährten Grundsatz „Information und Aufklärung vor Strafe“. Dies liegt unter anderem darin begründet, dass wir etwaige Umsetzungsdefizite im Datenschutz vor Ort vor allem als Informations- und Sensibilitätsdefizite hinsichtlich der beachtlichen Komplexität der Digitalisierung und der damit oft nur subtil erfolgenden Grundrechtseingriffe gegenüber Dritten erfahren. Wollen wir dem Datenschutz nützen, so gilt es exakt an dieser Stelle adressatengerecht und mit dem notwendigen Fingerspitzengefühl ein kognitives und auch emotionales Verständnis für die rechtsstaatliche, gesellschaftliche und individuelle Bedeutung dieses so wichtigen Themas zu initiieren.

So greifen wir seit Jahren den rechtlichen Impuls des noch geltenden Landesdatenschutz-gesetzes auf (§ 33 Abs. 2 und 3) und erfüllen ihn anhand der nachstehenden Bildungsmaßnahmen mit Leben. Mit Geltung der DS-GVO werden die entsprechenden Angebote auf der Grundlage des dortigen Art. 57 erfolgen.

Im Berichtszeitraum bezogen sich die oben genannten Bildungsmaßnahmen im öffentlichen Bereich und auch im Bereich der Privatwirtschaft zunehmend auf die DS-GVO.

So schulten wir die meisten Ministerien, einige von ihnen - dem jeweiligen aktuellen Umsetzungsstand der DS-GVO-Vorbereitungen angepasst - auch mehrmals.

Zudem führten wir mehrtägige Blockseminare an der Universität Rostock und an der Hochschule Wismar durch. Ergänzt wurden diese Angebote durch Vorlesungen an der Universität Greifswald und der Hochschule Neubrandenburg.

Des Weiteren erbringen wir ganz- oder auch mehrtägige Regelschulungen an der Verwaltungshochschule in Güstrow und im kommunalen Studieninstitut Mecklenburg-Vorpommern.

Darüber hinaus wandten wir uns mit gut angenommenen Schulungsangeboten an die oberen Landesbehörden (Landesämter), an Landkreisverwaltungen, an die Kommunalen Zweckverbände und an zahlreiche andere Landesverbände, Fachverbände und Vereinigungen wie zum Beispiel die IHK, an den Journalistenverband MV, an die Mitglieder der Liga der freien Wohlfahrtsverbände, an die Zahnärztekammer, die Akademie für Sozialmedizin MV oder auch das IQMV.

Im Rahmen dieser Angebote fokussieren wir uns - vor dem Hintergrund unserer nach wie vor (zu) knappen personellen Ressourcen - vor allem auf Multiplikatoren, die ihrerseits wieder zu einer entsprechenden Sensibilisierung in ihrem jeweiligen Wirkungskreis beitragen können und sollen.

Da sich die DS-GVO zum Beispiel in den Artikeln 8 und 12 explizit an die Kinder wendet, duldet nun die seit langem bestehende Forderung einer entsprechenden (Datenschutz-) Qualifizierung des Lehrpersonals an Schulen und Hochschulen keinen weiteren Aufschub mehr. So halten wir seit mehreren Jahren - immer noch völlig ungenügend abgerufene - Kooperationsressourcen für eine entsprechende Schulung der Lehramtsreferendarinnen/ -referendare und der Studierenden im Hochschulbereich (Uni Rostock) bereit.

Auf der Grundlage der bisherigen Erfahrungen gehen wir davon aus, dass der Wissens- und Sensibilisierungsbedarf aufgrund der weiterhin zunehmenden Digitalisierung nicht abnehmen wird - vielmehr ist im Gegenteil vor dem Hintergrund der mit der Digitalisierung einhergehenden enormen Grundrechtsrisiken künftig mit einem deutlichen Anstieg des Bedarfes zu rechnen. Diesem dringenden Bedarf wollen und werden wir im Rahmen unserer Möglichkeiten entsprechen.

4 Datenschutz und Bildung

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

Ausgehend von der bis heute uneingeschränkt gültigen Rechtsprechung des Bundesverfassungsgerichtes zum Grundrecht auf informationelle Selbstbestimmung und nach Artikel 57 Ziffer 1b der Europäischen Datenschutz-Grundverordnung (DSG-VO) ist es auch künftig eine der gesetzlichen Kernaufgaben unserer Behörde, über den Datenschutz und seine praktische Umsetzung in geeigneter Weise, das heißt zielgruppenorientiert, zeitnah und umfänglich, zu informieren. Ein besonderes Augenmerk gilt dabei spezifischen Angeboten für Kinder und Jugendliche.

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 jeder Einzelnen/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 demnach der Schlüssel für die Teilhabe und die Entwicklung einer aktiven und selbstbewussten Rolle in der Gesellschaft und für die Ausbildungs- und Erwerbsfähigkeit einer jeden Einzelnen/eines jeden Einzelnen unerlässlich.

„Digitale Selbstverteidigung“ ist für jede Bürgerin und jeden Bürger, der informationell selbstbestimmt sein und bleiben möchte, eine dringende Notwendigkeit. Darauf wiesen die Datenschutzbehörden des Bundes und der Länder bereits 2011 in einer Erklärung hin (siehe Beschluss der 82. Konferenz der Datenschutzbeauftragten vom 21. September 2011).

Die Kultusministerkonferenz schuf im Dezember 2016 mit der verabschiedeten Strategie „Bildung in der digitalen Welt“ eine Basis, die eng mit unserer Arbeit im Bildungsbereich korrespondiert. „Die Digitalisierung unserer Welt wird hier im weiteren Sinne verstanden als Prozess, in dem digitale Medien und digitale Werkzeuge zunehmend an die Stelle analoger Verfahren treten und diese nicht nur ablösen, sondern neue Perspektiven in allen gesellschaftlichen, wirtschaftlichen und wissenschaftlichen Bereichen erschließen, aber auch neue Fragestellungen zum Beispiel zum Schutz der Privatsphäre mit sich bringen.“ Den darin aufgezeigten Kompetenzrahmen, den „alle Schülerinnen und Schüler, die zum Schuljahr 2018/2019 in die Grundschule eingeschult werden oder in die Sek I eintreten, bis zum Ende der Pflichtschulzeit die in diesem Rahmen formulierten Kompetenzen erwerben können“, begrüßen wir ausdrücklich. Zudem stellte das Bundesministerium für Familie, Senioren, Frauen und Jugend einen 10-Punkte-Plan auf, der auf Grundlage der „Digitalen Agenda für eine lebensWerte Gesellschaft“ beruht. Dabei stehen digitale Kompetenzen und Teilhabe ebenso im Fokus wie diskriminierungsfreie Algorithmen.

Die Landesregierung Mecklenburg-Vorpommern bekennt sich ebenfalls zur „Kooperationsveinbarung zur Medienkompetenzförderung in MV“ und erkennt „eine besondere Herausforderung der Zukunft, die Digitalisierung der Gesellschaft, verantwortlich gestalten.“. [9] Nach alledem ist festzustellen, dass das Thema der Medienbildung und Medienkompetenzförderung in allen Ebenen angekommen ist.

[9] Koalitionsvereinbarung 2016 - 2021, Ziffer 215

Die Vermittlung von Datenschutzbewusstsein und Medienkompetenz ist nach unserer Auffassung eine gesamtgesellschaftliche Aufgabe. Im Einklang mit unserer gesetzlichen Aufgabe nach Artikel 57 Ziffer 1b DS-GVO stellen wir auch weiterhin einen wesentlichen Bereich der Medienbildungsangebote im Land und initiierten durch vernetztes Arbeiten ein umfangreiches Angebot mit zahlreichen Partnern und Institutionen.

4.1 Medienbildung/Medienkompetenzvermittlung

Die für Schulen, Lehrkräfte und Sozialpädagoginnen/Sozialpädagogen in der Regel kostenfreien Angebote unserer Behörde werden von den Einrichtungen gut angenommen. Die entsprechenden Anfragen nehmen stetig zu. Wie bereits im Zwölften Tätigkeitsbericht, Punkt 2, festgestellt, nehmen die Anfragen im Bereich der Erzieherinnen und Erzieher in Aus- und Weiterbildungsformaten ebenso zu wie Elternarbeit und Anfragen zahlreicher sozialer Träger. Dabei erstrecken sich die Angebote unserer Behörde mittlerweile von der Grundschule bis hin zu Berufsschulen. Unsere weiterhin zu sehr begrenzte personelle Kapazität führt dazu, dass die „Warteliste“ mittlerweile mindestens neun Monate beträgt.

Hinzu kommen Weiterbildungsformate aus dem Projekt „Medien-Familie-Verantwortung“, siehe Punkt 4.1.4., in denen bereits Termine bis 2020 geplant sind. In den Jahren 2016 und 2017 konnten Anfragen, trotz zusätzlicher Belastungen in unserer Behörde, siehe auch Punkt 4.1.3, nur erfüllt werden, wenn von den Anfragenden ein langer Wartezeitraum akzeptiert wurde. Hinzu kommt eine ständige Kooperation der Partner des „Medienaktiv MV“-Netzwerkes, siehe auch Punkt 4.1.2, bei Projekttagen vor Ort oder Formaten wie „Bildungsabende der Offenen Kanäle der Medienanstalt Mecklenburg-Vorpommern“ oder Unterstützung bei bundesweiten Projekten wie „webdays“ und landesweiten Formaten wie „Jugend im Landtag“ (*JiL*) und „Jugend fragt nach“ (*Jfn*) des Landesjugendrings Mecklenburg-Vorpommern. Als regelmäßig kooperierende Institutionen vor Ort sind vor allem zu nennen: Landeskoordinierungsstelle für Suchtthemen (*LAKOST*), die Medienanstalt Mecklenburg-Vorpommern (*MMV*) mit den Medientreckern und Offenen Kanälen, der Landesjugendring Mecklenburg-Vorpommern (*LJRMV*), das Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, das Landeskriminalamt Mecklenburg-Vorpommern (*LKA MV*) sowie die ComputerSpielschule Greifswald (*CSG*), das Filmbüro Wismar. Ohne die ganz wesentlichen Beiträge des „Medienaktiv MV“-Netzwerkes wäre eine so weitreichende Sensibilisierung und Schulung in unserem Bundesland nicht möglich.

Das Fazit bei allen Schulungen, Workshops und Veranstaltungen ist nach unseren Erkenntnissen und auf der Grundlage des Feedbacks der Teilnehmerinnen und Teilnehmer durchweg positiv. In den Datenschutz-Veranstaltungen ab der 5. Klasse geht es um die Gefahren im Netz, im Umgang mit den unterschiedlichen Medien sowie die technischen und rechtlichen Rahmenbedingungen (Persönlichkeitsrecht, Urheberrecht, Recht am eigenen Bild). Dabei verfolgen wir nicht den Ansatz der Reglementierung, sondern der gemeinsamen Exploration von Chancen und Risiken im Internet. Das Ziel unserer gemeinsamen Anstrengungen bleibt dabei grundsätzlich das Erlernen eines selbstbestimmten und informierten Umgangs mit digitalen Medien und Anwendungen. Denn nur wer die Chancen und Risiken unserer digitalen Gesellschaft kennt, kann diesen kompetent begegnen und eine informierte Entscheidung treffen.

Wir stellen vor dem Hintergrund der geschilderten Erfahrungen fest, dass ein steigendes Interesse an der Begleitung der Ausbildung von Erzieherinnen und Erziehern, der Weiterbildung von Erzieherinnen und Erziehern in den Kindertagesstätten, im Hort und von Lehrkräften im Grundschulbereich besteht. Dabei geht es nicht nur um die rechtliche Betrachtung des Datenschutzes, sondern ebenso um die Medienbildung/Medienkompetenzvermittlung im sogenannten frühkindlichen Bereich. Häufig werden im gleichen Kontext Anfragen zur Elternarbeit in diesem Bereich aufgegriffen bzw. gleich mit einem thematischen Elternabend in KITA, Hort, Grundschule oder Orientierungsstufe kombiniert.

4.1.1 Projekte „Medienscouts M-V“ und „TEO - Protect Privacy“

Projekt „Medienscouts MV“

Der Projektstart erfolgte bereits im Juni 2012. Das „Medienscouts MV“-Projekt wird seither unterstützt von der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern (*LAKOST*), dem Landesjugendring Mecklenburg-Vorpommern (*LJRMV*), dem Landeskriminalamt (*LKA)*, der Medienanstalt Mecklenburg-Vorpommern (*MMV*) und deren Online-Selbsthilfeplattform juuuport sowie der Computerspielschule Greifswald *(CSG*) vom Medienzentrum Greifswald e. V.

Auch im Berichtszeitraum wurden die Ausbildungswochenenden für Medienscouts MV fortgeführt. Das Konzept der Ausbildungswochenenden hat sich etabliert. Neben den thematischen Workshops zum Umgang mit digitalen Medien haben wir verstärkt auf die methodische Ausbildung den Fokus gelegt, sodass die Jugendlichen in der Lage sind, Workshops, Vorträge und Projekttage thematisch und methodisch umzusetzen. Weiterhin steht ihnen das Expertenteam im Nachgang der Ausbildung dauerhaft zur Verfügung, um Hilfe und Unterstützung zu leisten. 2016 fanden die Ausbildungswochenenden in Güstrow und Waren/Müritz statt und 2017 in Wismar und Greifswald.

Einmal jährlich werden alle bereits ausgebildeten Medienscouts MV zu einem Update-Treffen eingeladen, um sich auszutauschen, neue Themen zu besprechen und Trends zu diskutieren.

Im Jahr 2017 haben wir ein Treffen für Lehrerinnen und Lehrer sowie Schulsozialarbeiterinnen und Schulsozialarbeiter unter dem Motto „Medienscouts MV machen Schule“ organisiert. Dies hat den Bekanntheitsgrad der Medienscouts MV gesteigert und vor allem geholfen, dass neue Regionen in Mecklenburg-Vorpommern erschlossen wurden. Dabei gibt es allerdings immer noch Regionen, in denen es keine Medienscouts MV gibt. Die Kapazitäten für ein Wochenende sind jedoch begrenzt. Derzeit existiert eine entsprechende Warteliste.

Bisher wurden in elf Ausbildungswochenenden seit 2012 mehr als 270 Medienscouts MV landesweit ausgebildet. Das Projekt findet an wechselnden Orten statt, um auf mittlere Sicht eine gerechte regionale Verteilung und auf die Teilnehmer bezogene Erreichbarkeit des Projektes zu gewährleisten. Durch den peer-to-peer-Ansatz ist es dem Gemeinschaftsprojekt eigen, dass das erworbene und verfestigte Wissen multipliziert wird. Somit wurden ca. 13.000 Schülerinnen und Schüler in den vergangenen fünf Jahren durch die Medienscouts MV erreicht.

In einigen Schulen, vor allem dort, wo es auch erwachsene Medienscouts MV gibt (meist Schulsozialarbeiterinnen und Schulsozialarbeiter), wurden nachmittägliche „Medienscouts MV *AG's*“ eingerichtet, die sich regelmäßig treffen. Dies bedeutet für die Jugendlichen und für die Schulsozialarbeiterinnen und Schulsozialarbeiter einen erheblichen Zusatzaufwand. Uns sind Schulen bekannt, an denen eine hohe Wertschätzung und Anerkennung für dieses ehrenamtliche Engagement gepflegt wird. Dies gilt unseres Wissens jedoch nicht für alle Schulen.

Der Erfolg dieses bundesweit beachteten Projektes setzt auch weiterhin voraus, dass mindestens die strukturelle, organisatorische und wirtschaftliche Basis für diese außerschulische Kooperation erhalten bleibt und sich finanziell marktorientiert entwickelt. Wünschenswert wären für die Zukunft die Erstellung einer datenschutzgerechten Messanger-App (nicht nur für die Medienscouts MV) und eine den steigenden Kosten angepasste bessere finanzielle Grundausstattung der Medienprojekte.

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.

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

„Tage ethischer Orientierung“ ist ein schulkooperatives Modell der Nordkirche, das in Kooperation mit unserer Behörde durchgeführt wird. Dieses 4-tägige Modul ist speziell für die 5. und 6. Klassen konzipiert. Es geht darum, Inhalte der Handlungsfelder „Datenspuren im Netz, soziale Netzwerke, Cybermobbing, Apps, Smartphones, Handys und Computerspiele“ mit den Grundrechten nach Art. 1 und 2 des Grundgesetzes (GG) abzuwägen und damit Möglichkeiten verantwortlicher Nutzung digitaler Medien zu erarbeiten und mit Blick auf die eigene Praxis zu reflektieren.

Es handelt sich hier ebenfalls gemäß „unserer Tradition“ um ein Gemeinschaftsprojekt. So unterstützen im Rahmen dieses ebenfalls überregional bekannten Projektes Referenten der *LAKOST MV*, des Kompetenzzentrums und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern sowie der ComputerSpielSchule das Projekt inhaltlich.

Bisher wurden seit 2013 rund 500 Schülerinnen und Schüler der 5. und 6. Klassen sowie Lehrerinnen und Lehrer in Mecklenburg-Vorpommern geschult. In jedem Durchgang werden zwischen drei bis vier 5. und 6. Klassen sowie die jeweiligen begleitenden Lehrerinnen und Lehrer erreicht.

Beide Projekte sind sehr erfolgreich und sollen fortgeführt werden. Hierzu bedarf es für die bekannten außerschulischen Partner verlässlicher finanzieller und personeller Rahmenbedingungen. Die Verzahnung von weiteren Projekten wie „Jugend im Landtag“, „Jugend fragt nach“ oder „Jugend hackt“ oder dem Schülerzeitungsprojekt (LISZ) funktioniert durch die bereits vorhandene Netzwerkarbeit sehr gut, siehe auch Punkt 4.1.2.
Interessierte können sich informieren unter: www.medienscouts-mv.de und www.teoinmv.de.

4.1.2 Netzwerk „Medienaktiv M-V“

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

Nach unserer Kenntnis aus bundesweiten Arbeitsgruppen sind auch die anderen Bundesländer auf dem Weg, sich institutionsübergreifend zu vernetzen und Konzepte wie „Medienbildung in Thüringen 2020“ oder „Bayern digital“ aktiv voranzutreiben, um das Thema der Medienbildung und Medienkompetenzvermittlung möglichst schnell und flächendeckend umzusetzen. Wir unterstützen diesen Wissenstransfer aktiv, sodass andere Bundesländer von unseren Kenntnissen und der Zusammenarbeit profitieren. Möchte das Land Mecklenburg-Vorpommern jedoch weiterhin die jetzige bundesweite Vorreiterrolle behalten, bedarf es entsprechender Maßnahmen der Landesregierung, siehe Punkt 4.1.5.

In der Präambel des „Medienaktiv MV“ haben wir uns bereits 2013 das Ziel gesetzt „den Dialog mit Politik zu fördern“. Auf Initiative unserer Behörde hat sich das Netzwerk im Jahr 2016 mit der Landtagswahl diesem Ziel intensiver angenommen. So haben wir „Medienpolitische Forderungen an die zukünftige Arbeit der Landespolitik“ erarbeitet und sie öffentlich auf der Frühjahrstagung „Medienaktiv meets Politik“ des Netzwerkes am 31. März 2016 diskutiert. Nachdem wir in Fachkreisen des Netzwerkes essentielle Themen exploriert hatten, sollte der 1. Medienpolitische Abend mit Landtagsabgeordneten, Vertretern aus Politik und Verwaltung sowie den jeweiligen Zielgruppen, beispielsweise Erzieherinnen und Erziehern oder Lehrerinnen und Lehrern, in gemeinsamen Forderungen münden. Der 1. Medienpolitische Abend wurde breit angenommen. Auf der anschließenden Frühjahrstagung „Medienaktiv meets Politik“ wurden die Forderungen des Netzwerkes dann mit Vertretern der seinerzeit vier demokratischen Fraktionen des Landtages diskutiert.

Im Rahmen des 2. Medienpolitischen Abends im Januar 2017 wurden erneut die Möglichkeiten der strukturellen Unterlegung von Angeboten der Medienkompetenzerwerbung in der Lehrerfortbildung und in der Sozialpädagogikausbildung diskutiert.

Das Netzwerk macht die Vielfalt der Medienangebote in Mecklenburg-Vorpommern besser wahrnehmbar. Wir sehen uns als Partner im Bereich der Medienbildung in Mecklenburg-Vorpommern, um Erfahrungen oder Potentiale einbringen zu können.

Künftig ist eine weitere Vernetzung mit dem Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern geplant. Das Netzwerk „Medienaktiv MV“ wird auch weiterhin alle neuen Kenntnisse und Entwicklungen, weitere Kooperationen und möglichen Schritte zur grundrechtsverträglichen Umsetzung der Digitalisierung unserer Gesellschaft aufgreifen, um die gesellschaftliche Teilhabe, Demokratiebildung und Chancengleichheit zu fördern.

Dies wird in dem Dialog mit Politik ebenfalls erörtert wie mögliche Arbeitsfelder und Aufgaben in die Kooperationsvereinbarung zur Medienkompetenzförderung in Mecklenburg-Vorpommern einfließen zu lassen, siehe Punkt 4.1.3.

Das Netzwerk „Medienaktiv MV“ nimmt einen hohen Stellenwert im Bereich der Medienbildung in Mecklenburg-Vorpommern ein. Der Bekanntheitsgrad wächst stetig. Dies führt zu einem Anstieg der entsprechenden Unterstützungsanfragen. So gilt es künftig auch, die im Netzwerk und in den Gesprächen aufgekommene Frage nach einer unabhängigen, neutralen und vernetzenden Stelle intensiv zu prüfen.

4.1.3 Kooperationsvereinbarung zur Medienkompetenzförderung

Die Landesregierung Mecklenburg-Vorpommern räumt der Förderung von Medienbildung und Medienkompetenz einen erkennbaren Stellenwert ein. Mit der „Kooperationsvereinbarung zur Medienkompetenzförderung in Mecklenburg-Vorpommern“ gibt sie Impulse für eine vertiefte Zusammenarbeit zwischen medienpädagogischen Einrichtungen, Schulen sowie Kinder- und Jugendeinrichtungen. Aufgrund unserer breit aufgestellten Bildungsangebote und der entsprechend vernetzten Bildungspraxis im Land ist unsere Behörde ebenfalls Unterzeichner diese Vereinbarung. Kooperationspartner sind die Staatskanzlei des Landes Mecklenburg-Vorpommern, das Ministerium für Inneres und Sport M-V, das Ministerium für Bildung, Wissenschaft und Kultur M-V, das Ministerium für Arbeit, Gleichstellung und Soziales M-V, der Landesbeauftragte für Datenschutz und Informationsfreiheit M-V sowie die Medienanstalt M-V. In der Vereinbarung heißt es an exponierter Stelle: „Medienbildung ist eine Zukunftsaufgabe unseres Landes, Medienkompetenz eine notwendige Schlüsselkompetenz für alle Menschen in unserer Gesellschaft. Allen Bürgerinnen und Bürgern soll die Möglichkeit gegeben werden, sich umfangreiches Wissen über heutige Medien anzueignen und ihre Kompetenzen hierbei kontinuierlich weiterzuentwickeln.“

Aus der Kooperationsvereinbarung gehen mehrere Aufgabenschwerpunkte hervor, die während der Laufzeit der Kooperationsvereinbarung umgesetzt werden sollen. Durch die Umstrukturierung nach der Landtagswahl 2016 kam es durch die Veränderung von ministeriellen Zuständigkeiten zu Verzögerungen sowohl in den Arbeitsgruppen als auch in den Abstimmungsrunden. Nachdem diese geklärt werden konnten, wurde die begonnene Arbeit fortgesetzt. Aktuell wird die Kooperationsvereinbarung evaluiert und der Erfahrungsbericht soll dem Kabinett im Herbst 2018 vorgelegt werden.

Mittlerweile haben sich andere Bundesländer nach dem Vorbild in Mecklenburg-Vorpommern auf den Weg gemacht, ebenfalls Kooperationsvereinbarungen zur Medienkompetenz zu schließen. So wurde beispielsweise in Thüringen die erste „Kooperationsvereinbarung zur nachhaltigen Weiterentwicklung von Medienkompetenz in Thüringen“ im Februar 2017 unterschrieben, die unseres Wissens in Anlehnung an die Kooperationsvereinbarung im Mecklenburg-Vorpommern entwickelt wurde. Dies ist ein Ergebnis der vernetzenden Arbeit unserer Behörde auch über die Landesgrenze hinaus. Da dies eine gesamtgesellschaftliche Aufgabe ist, kann sie nicht einem Ressort zugeteilt werden.

Die ressortübergreifende und vernetzende Arbeit mit Medienaktiv M-V ist daher unverzichtbar wichtig. Eine Fortführung und Neuschreibung der Kooperationsvereinbarung in Mecklenburg-Vorpommern ist aus unserer Sicht wünschenswert und notwendig. Darin sollen noch nicht beendete Ziele sowie gegebenenfalls neue und weiterführende Aufgaben klar benannt werden.

Durch die jetzige Kooperationsvereinbarung zur Medienkompetenzförderung in M-V sind zwei Arbeitsgruppen gegründet worden, die sich folgenden Aufgabenbereichen und Herausforderungen stellen:

4.1.3.1 Arbeitsgruppe „*KITA*“/AG Frühkindliche Medienbildung

Vor dem Hintergrund mehrjähriger Erfahrung vor Ort konnten wir einen steigenden Schulungsbedarf vor allem im Kindergarten-, Hort- und Grundschulbereich feststellen. Aus diesem Grund wurde in der Kooperationsvereinbarung zur Medienkompetenzförderung in Mecklenburg-Vorpommern die Arbeitsgruppe „KITA“ initiiert. Die Arbeitsgruppe wird durch die Vertragspartner unter Federführung des fachlich zuständigen Bildungsministeriums initiiert und wechselte nach der Landtagswahl im Herbst 2017 in das Sozialministerium. Fachlich wird die Arbeitsgruppe durch Vertreterinnen der LIGA der Spitzenverbände der Freien Wohlfahrtspflege in Mecklenburg-Vorpommern e. V., Vertreterinnen von Kindertagesstätten, der Medienanstalt Mecklenburg-Vorpommern, der Landeskoordinierungsstelle für Suchtthemen MV (LAKOST), dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin, der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, Universität Greifswald (Lehrstuhl für Religions- und Medienpädagogik) und unserer Behörde unterstützt.

Nach der konstituierenden Sitzung wurde die Notwendigkeit klar, einen gemeinsamen Medienbegriff und eine gemeinsame Definition von Medienbildung im frühkindlichen Bereich zu erarbeiten. Nun folgend werden einzelne Themenblöcke wie Stärkung von Primärerfahrungen (Zuarbeit Diakonie + DRK/LIGA), Aufklärung, Prävention, Elternarbeit (Zuarbeit LAKOST + Kompetenzzentrum) und Medienangebote für Kinder von 0- bis 10 Jahren (Zuarbeit MMV + LfDI MV) ausgearbeitet. Die Universität Greifswald soll die wissenschaftliche Begleitung übernehmen.

Nicht nur die oben genannten eigenen Erfahrungen und Anfragen, sondern auch die Ergebnisse der miniKIM 2014[10] und der DIVSI U9[11] Studien belegen einen steigenden Bedarf zu Schulungs- und Informationsmaßnahmen nicht nur bei Erzieherinnen und Erziehern sowie Ausbilderinnen und Ausbildern, sondern auch bei den Kindern selbst, da die Studienlage zudem eine zunehmende Mediennutzung bei immer jüngeren Kindern nachweist.

Medienbildung im frühkindlichen Bereich möchten wir jedoch nicht in der Form verstanden wissen, dass es zum Beispiel „Tablet-Gruppen“ für 3- oder 4-Jährige geben sollte. Vielmehr sollen die in diesem Alter schon (und noch) gut vorhandenen Möglichkeiten genutzt werden, an die kognitiven, motorischen und senso-motorischen Erfahrungen der Kinder anzuknüpfen und ihnen so erklärbar zu machen, was in den Medien und anschließend mit ihnen „passiert“ und wie dies alles funktioniert.

[10] http://www.mpfs.de/?id=565
[11] https://www.divsi.de/publikationen/studien/divsi-u9-studie-kinder-der-digitalen-welt/

So kann und sollte der erste kritische Blick auf digitale Medien begleitet werden, der die Wahrscheinlichkeit erhöht, fortführend ein gesundes Maß an Nutzung, Verstehen von Inhalten und Wirkungsweisen zu ermöglichen. Medienkompetenzvermittlung im frühkindlichen Bereich verstehen wir als Medienbildung für Kinder, Eltern sowie Erzieherinnen und Erzieher, mit dem Ziel der Anleitung einer sinnvollen, geregelten, zeit- und altersangemessenen, kreativen und begleiteten Nutzung. Als nicht sinnvoll erfahren wir das Bild einer polarisierenden Konkurrenz zwischen digitalen Medien und nicht-digitalen Medien, siehe Punkt 4.1.4.

4.1.4 Kampagne „Medien- Familien-Verantwortung“

Ausgehend von wissenschaftlichen Untersuchungen ist ein weiteres Gemeinschaftsprojekt in Mecklenburg-Vorpommern entstanden. Zunächst startete dies im Herbst 2016 mit der Plakatkampagne „Heute schon mit Ihrem Kind gesprochen?“

Das Ziel der Plakatkampagne ist es, Eltern dahingehend zu sensibilisieren, dass sie darüber nachdenken, wie oft sie mit dem Smartphone beschäftigt sind und ihre Kinder ignorieren. Der Landkreis Rostock war bereits mit einem Plakatmotiv 2016 zur Kinderschutzwoche regional aktiv. Diese Idee wurde an die Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern *(LAKOST)* herangetragen. Danach bildete sich ein Gemeinschaftsprojekt mit

- der Landesfachstelle Familienhebammen in Mecklenburg-Vorpommern,
- dem Landesdatenschutzbeauftragten Mecklenburg-Vorpommern,
- der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern,
- dem Ministerium für Soziales, Integration und Gleichstellung Mecklenburg-Vorpommern,
- der Landeskoordinierungsstelle Bundesinitiative Netzwerke Frühe Hilfen und Familienhebammen, Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern, Abteilung Jugend und Familie,
- dem Kompetenzzentrum und Beratungsstelle für exzessiven Mediengebrauch und Medienabhängigkeit,
- dem Beratungs- und Therapiezentrum Ludwigslust/Parchim,
- den Frühe Hilfen der Hansestadt Rostock und des Landkreises Ludwigslust-Parchim und
- dem Ministerium für Wirtschaft, Arbeit und Gesundheit Mecklenburg-Vorpommern.

Die Koordination des Projektes liegt bei der *LAKOST*. Gemeinsam wurden zwei weitere Plakatmotive sowie eine City Card entworfen und landesweit verteilt. Die Plakate wurden deutschlandweit angefragt. Nach der Klärung der Vervielfältigungsrechte konnten anderen Institutionen, zuständigen Ressorts und Initiativen die Motive zur Verfügung gestellt werden, sodass die Plakatmotive mittlerweile deutschlandweit bekannt sind.

Viele Eltern sind sich ihrer misslichen Vorbildfunktion in Sachen Handykonsum nicht genügend bewusst. Hier setzt das Projekt an. Gekoppelt wurde dies mit einer Informationskampagne über die Verbreitung von Studienergebnissen und von grundlegendem Wissen sowie Aufklärung über Gefahren des Smartphone- und Medienkonsums für die Bindung zwischen Bezugspersonen und Kindern. Im weiteren Verlauf wurde es mit Unterstützung des Verbandes der Ersatzkassen e. V. (*vdek e. V.*) 2017 möglich, eine Fortbildungsreihe für Erzieherinnen und Erzieher zu konzipieren, die im Januar 2018 starten wird. Unsere Behörde ist intensiv an der Vorbereitung und Durchführung der modularen Fortbildung beteiligt.

Diese Weiterbildungsreihe wäre jedoch ohne die Finanzierung durch den Verband der Ersatzkassen nicht möglich. Auch hier liegt die Projektleitung beziehungsweise Koordination in den Händen der *LAKOST*. Projektpartner sind unsere Behörde (*LfDI MV*), das Kompetenzzentrum und Beratungsstelle für exzessiven Mediengebrauch und Medienabhängigkeit, das Medienzentrum Greifswald e. V., die Medienwerkstatt Identity Films e. V., die Regionale Arbeitsstelle für Bildung, Integration Mecklenburg-Vorpommern e. V. und die Bildungsstätte Schabernack, Zentrum für Praxis und Theorie der Jugendhilfe, Güstrow.

In acht Modulen werden unter anderem Themen wie Einflüsse der Medienaneignung, Mediennutzung in den Familien, Aufgreifen von Medienerlebnissen in der Kita sowie motivierende Elterngespräche behandelt und medienpädagogische Angebote entwickelt. Es gibt bereits eine Warteliste für das Jahr 2019.

4.1.5 Ausblick/Fazit

Das bisherige Maßnahmepaket und die Projekte, die mit Unterstützung bzw. unter Federführung des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern ins Leben gerufen wurden, sollen weitergeführt werden. Nach internationalen Vergleichsstudien droht Deutschland, und hier insbesondere auch Mecklenburg-Vorpommern, den digitalen Anschluss zu verlieren. Dies wäre für die wirtschaftliche Perspektive und auch für das Grundrechtsbewusstsein unserer Bevölkerung eine ganz wesentliche Belastung.

Medienbildung ist eine gesamtgesellschaftliche Aufgabe, die Demokratiebildung, Teilhabe und Chancengleichheit verbindet, um eine „digitale Spaltung der Gesellschaft“ aufzuhalten. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern leistet einen umfangreichen Beitrag für diese gesamtgesellschaftliche Aufgabe. Jedoch unter Zugrundelegung der Kooperationsvereinbarung zur Medienkompetenzförderung in Mecklenburg-Vorpommern, den geltenden gesetzlichen Rahmenbedingungen und den „Medienpolitischen Forderungen an die zukünftige Arbeit der Landespolitik“ ergeben sich weiterhin folgende Handlungsbereiche, die durch einen politischen Willen in der Landesregierung umzusetzen sind:

- die weitere Unterstützung für die Vernetzung möglichst aller medienpädagogisch Wirkenden in Mecklenburg-Vorpommern und die Stärkung des Netzwerkes „Medienaktiv MV“ in allen beschriebenen Handlungsfeldern,
- die verstärkte Einbindung von Familienarbeit zur Stärkung der Medienkompetenz,
- die niederschwellige Ermöglichung von konstruktiv-kritischer Medienbildung, angefangen bei der frühkindlichen Bildung und verstanden als lebenslanges Lernen, das sich wie ein roter Faden durch viele Bildungsangebote zieht,
- die 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, 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.

Gegenwärtig wird die Medienbildung in Mecklenburg-Vorpommern ungewöhnlich stark von außerschulischen Partnern getragen - ein nicht unbedingt negativer Aspekt. Zur Stabilisierung und zur Sicherung von Nachhaltigkeit bedarf es jedoch planbarer und verlässlicher Rahmenbedingungen der Partner, um mittel- und langfristig eine flächendeckende Medienbildung in unserem Bundesland zu sichern. Dies ist nach unserer Überzeugung bisher noch nicht ausreichend umgesetzt.

Wir empfehlen der Landesregierung daher, 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. [12]

5 Technik und Organisation

5.1 Neue Technologien

5.1.1 Das Standard-Datenschutz-Modell

Das Standard-Datenschutzmodell (*SDM*) ist eine Methode zur Datenschutz-Beratung und Datenschutz-Prüfung auf der Basis der Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit. Es unterstützt die Transformation gesetzlicher Anforderungen in technische und organisatorische Maßnahmen bei personenbezogenen Verfahren. Das verbessert insbesondere die Integrität und Transparenz von Datenschutz-Beratungen und Datenschutz-Prüfungen und ermöglicht es Verantwortlichen, die Verarbeitung personenbezogener Daten datenschutzkonform auszugestalten.

Über das SDM haben wir im Zwölften Tätigkeitsbericht unter Punkt 4.1.1 bereits ausführlich berichtet. Inzwischen hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) die Version 1.0 des SDM im November 2016 als sogenannte Erprobungsfassung verabschiedet und dessen evaluierende Anwendung empfohlen. Der Arbeitskreis Technik der Datenschutzkonferenz, AK Technik siehe Punkt 8, wurde beauftragt, das SDM weiterzuentwickeln und insbesondere den Katalog mit Referenz-Schutzmaßnahmen zur Umsetzung der sieben Gewährleistungsziele zu erarbeiten.

[12] Kooperationsvereinbarung zur Medienkompetenzförderung in M-V https://www.datenschutz-mv.de/presse/2015/koop-teo.pdf

Die Weiterentwicklung des SDM erfolgt insbesondere vor dem Hintergrund der am 25. Mai 2016 in Kraft getretenen Europäischen Datenschutz-Grundverordnung (*DS-GVO*). Sie enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. In Art. 5 DS-GVO werden wesentliche Grundsätze für die Verarbeitung personenbezogener Daten formuliert: Die Verarbeitung muss rechtmäßig, nach Treu und Glauben, nachvollziehbar, zweckgebunden, auf das notwendige Maß beschränkt, auf der Basis richtiger Daten, vor Verlust, Zerstörung und Schädigung geschützt und die Integrität und Vertraulichkeit wahrend stattfinden. Das SDM bietet geeignete Mechanismen, um diese rechtlichen Anforderungen der DS-GVO in technische und organisatorische Maßnahmen zu überführen. Da das SDM zunächst mit Blick auf die Datenschutzgesetze von Bund und Ländern entwickelt wurde, sind insbesondere begriffliche Anpassungen an die DS-GVO erforderlich. Beispielsweise muss der für die DS-GVO zentrale Begriff des Risikos (für die Rechte und Freiheiten natürlicher Personen) im SDM verankert und mit dem dort bisher verwendeten Begriff des Schutzbedarfs in ein sinnvolles Verhältnis gebracht werden.

Wenn diese grundlegenden Anpassungen des SDM an die DS-GVO abgeschlossen sind, wird die Erarbeitung der einzelnen Bausteine für den Referenz-Maßnahmenkatalog fortgesetzt. Es liegen bereits zahlreiche Bausteine im Entwurf vor, die nach Fertigstellung durch den AK Technik dann nach und nach veröffentlicht werden.

Das SDM steht in einer engen Beziehung zur Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (*BSI*)[13]. Der vom BSI entwickelte IT-Grundschutz ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium konkrete Anforderungen. Die Umsetzung dieser Sicherheitsmaßnahmen ist für den Datenschutz nach wie vor essentiell. Aber die Zielrichtung von BSI-Grundschutz und SDM unterscheiden sich ganz wesentlich. Im Unterschied zum Grundschutz nimmt das SDM die Schutzperspektive Betroffener ein und fokussiert sich primär auf die Minderung der Intensität des Grundrechtseingriffs. Es betrachtet erst in einem zweiten Schritt die Grundrechtsverletzungen, die beispielsweise durch eine mangelhafte IT-Sicherheit entstehen können. In der Vergangenheit enthielt der Baustein 1.5 (Datenschutz) lediglich 16 Maßnahmen zum Datenschutz. Angesichts der mehr als 1.000 Maßnahmen zu Fragen der IT-Sicherheit war offensichtlich, dass Datenschutzaspekte im IT-Grundschutz völlig unterrepräsentiert dargestellt worden waren. Im Rahmen der Modernisierung der Grundschutzmethodik durch das BSI wurde auch das Verhältnis von Datenschutz und Informationssicherheit neu justiert. Im neuen BSI-Standard 200-2[14] wird auf das SDM verwiesen, wenn es darum geht, das Risiko eines Grundrechtseingriffs, und daraus folgend des Schutzbedarfs, zu bestimmen.

[13] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.html

Das neue Grundschutz-Kompendium, das die Grundschutzkataloge ersetzt, enthält im Bereich „CON: Konzeption und Vorgehensweisen“ den neuen Baustein „CON.2 Datenschutz“[15], der die Abgrenzung zwischen Informationssicherheit und Datenschutz beschreibt und als Maßnahme CON.2.A1 die Umsetzung des SDM empfiehlt.

Das SDM ist auch ein geeignetes Werkzeug, um einerseits die in der DS-GVO geregelten Zertifizierungsverfahren (siehe Art. 42 ff.) zu strukturieren und um andererseits die in Art. 35 DS-GVO beschriebene Datenschutz-Folgenabschätzung (*DSFA*) zu unterstützen. In einem DSFA-Planspiel zu einem hypothetischen Beispielsfall eines „Pay as you drive“-Verfahrens[16] haben wir gemeinsam mit unseren Kolleginnen und Kollegen vom ULD Schleswig-Holstein gezeigt, dass das SDM eine Datenschutz-Folgenabschätzung sehr effektiv unterstützt. Das SDM trägt maßgeblich dazu bei, die Beeinträchtigungen und Risiken für die Rechte und Freiheiten für die betroffenen Personen, die von der jeweiligen Datenverarbeitung ausgehen, vollständig zu betrachten und zu bewerten. Die Anwendung des SDM bei der Erstellung einer DSFA ermöglicht es somit dem Verantwortlichen, die in Art. 35 Abs. 1 DS-GVO geforderte Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge vollständig vorzunehmen.

Die Weiterentwicklung des SDM und die Erarbeitung des Referenz-Maßnahmenkatalogs wird sicher noch eine längere Zeit in Anspruch nehmen. Dennoch kann und sollte die Anwendung des SDM schon jetzt erprobt werden. Das Kapitel 7 des SDM enthält einen generischen Maßnahmenkatalog, der solange zur Auswahl von Einzelmaßnahmen genutzt werden kann, bis die Referenz-Maßnahmenkataloge vorliegen.

Um auf dem aktuellen Stand zu SDM bleiben zu können, empfehlen wir den Bezug des SDM-Newsletters[17]. 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, 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.

15 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_2_Datenschutz.html

16 https://www.datenschutz-mv.de/datenschutz/DS%E2%80%93GVO/Hilfsmittel-zur-Umsetzung

17 https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

5.1.2 E-Government mit modernen Kommunikationsstandards

Öffentliche Stellen müssen im Rahmen von E-Government-Verfahren sicher miteinander kommunizieren. Hierfür sind geeignete Standards unabdingbar. *OSCI*-Transport, siehe Elfter Tätigkeitsbericht, Punkt 4.5, und *XTA, XÖV*-Transport-Adapter siehe Zwölfter Tätigkeitsbericht, Punkt 4.1.5, sind solche Standards. *OSCI*-Transport ist ein Standard für einen sicheren Transportdienst für Nachrichten an öffentliche Stellen, *XTA* hingegen kommt die Rolle eines Zubringer-Protokolls zu, welches Fachverfahren auf sichere Weise mit der *OSCI*-Infrastruktur verbindet.

Im Berichtszeitraum wurde im Standard *OSCI*-Transport Version 1.2 eine schwerwiegende Sicherheitslücke gefunden und geschlossen. Nutzerinnen und Nutzer hätten unter Ausnutzung dieser Lücke unbefugt auf Inhalte verschlüsselter Kommunikation anderer Nutzerinnen und Nutzer zugreifen können. Der Kreis möglicher Angreifer war jedoch beschränkt auf solche öffentlichen Stellen, die sich gegenüber den anderen Kommunikationspartnern authentisieren können (siehe auch https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k17-1100.html). Der Standard wurde daraufhin korrigiert und den Betreibern von E-Government-Verfahren und -Infrastruktur-Komponenten wurden Patches (Korrekturen) für die hierfür benutzte Software zur Verfügung gestellt.

Es zeigte sich jedoch, dass die Verantwortung für die Korrekturen an den Standards *OSCI*-Transport und *XTA* und deren Implementationen teils unklar und teils unzweckmäßig verteilt sind. Datenschutzrechtlich verantwortlich für den sicheren Versand von Nachrichten ist die absendende Institution. Sie bedient sich bei Verwendung von *OSCI*-Transport und *XTA* in der Regel eines zentralen Informationstechnik-Dienstleisters. Im vorliegenden Fall kann nur dieser Dienstleister die Patches einspielen und die Konfiguration der zentralen Komponenten anpassen. Die Pflege und Weiterentwicklung der Standards *OSCI*-Transport und *XTA* obliegt hingegen der Koordinierungsstelle für IT-Standards (*KoSIT)* im Auftrage des IT-Planungsrates. Spezialisierte Firmen implementieren die Standards in Software und aktualisieren die Programme, wenn sich die Standards ändern. Unklar ist nun, inwieweit *KoSIT* bzw. IT-Planungsrat rechtlich bindend verpflichtet sind, die Standards und auch deren Implementationen auf dem aktuellen Stand von Informationssicherheit und Datenschutz zu halten. Die Nutzerinnen und Nutzer von Infrastrukturen nach den genannten Standards benötigen außerdem geeignete Auditierungsschnittstellen, über die sie sich im laufenden Betrieb von der ordnungsgemäßen Funktion der Infrastrukturkomponenten nach diesen Standards überzeugen können.

Wir haben diese Probleme der *KoSIT* im letzten Berichtszeitraum vorgestellt. Eine verbindliche Lösung steht jedoch aus.
Dennoch sind *OSCI*-Transport und *XTA* zur sicheren Kommunikation öffentlicher Stellen untereinander auch gegenwärtig gut geeignet. Der IT-Planungsrat, siehe Punkt 7, hat in seiner 22. Sitzung im März 2017 den dauerhaften Betrieb der aktuellen Fassung von *XTA* (*XTA 2*) beschlossen und alle Fachministerkonferenzen gebeten, den Einsatz von *XTA* in ihren jeweiligen Bereichen zu prüfen (Beschluss 2017/06). Auch wir erneuern deshalb ausdrücklich unsere Empfehlungen zugunsten von *OSCI*-Transport und *XTA*, denn öffentliche Stellen unseres Landes nutzen *OSCI*-Transport und *XTA* bislang selten.

5.1.3 Datenschutz im Internet der Dinge

Im Zeitalter der Digitalisierung taucht immer häufiger das Schlagwort „Internet der Dinge“, kurz IoT, engl. „Internet of Things“, auf. Während in der Vergangenheit der klassische Personalcomputer immer mehr von „smarten“ portablen Geräten ersetzt wurde, beispielsweise dem Smartphone oder Tablet, zeichnet sich nunmehr der Trend ab, dass auch klassische Gegenstände des Alltags „zum Leben erwachen“. So werden beispielsweise Kühlschränke, Fernseher, Brillen oder selbst Zahnbürsten mit Prozessoren, Sensoren und Netzwerktechnik ausgestattet. Sie sind in der Lage, andere vernetzte Geräte zu erkennen und nicht mehr nur mit ihren Nutzerinnen und Nutzern, sondern auch untereinander - ggf. sogar weltweit - zu kommunizieren und Aufgaben eigenständig durchzuführen.

Ein recht bekanntes Beispiel für typische Produkte des Internet der Dinge, inzwischen soll es über 8 Milliarden von ihnen geben, sind die sogenannten Wearables. Hierbei handelt es sich im einfachsten Fall um schmale Fitnessarmbänder, aber inzwischen auch um funktionell umfangreich ausgestattete digitale Uhren, sogenannte Smartwatches. Diese Geräte haben einen beeindruckenden Funktionsumfang. Schon die einfachsten Geräte können mehr als nur die Uhrzeit anzuzeigen, unter anderem den Fitnesszustand überwachen, Details über den Schlaf aufzeichnen und Daten über den Herzschlag sammeln. Sie zeigen den Nutzerinnen und Nutzern ihre Hochs und Tiefs, neue sportliche Rekorde und sollen die Nutzerinnen und Nutzer dadurch motivieren, dass sie die Rekorde dann auch noch über soziale Netzwerke mit anderen teilen können. Einige Modelle können zudem Musik abspielen, Nachrichten vom Handy anzeigen, den Standort anzeigen oder sogar die Umgebung mit einer kleinen Kamera mehr oder weniger heimlich filmen.

Im Zusammenhang mit dem Internet der Dinge fällt in der letzten Zeit auch immer öfter der Begriff des sogenannten Smart Home. Auch die internetfähigen Geräte im Haushaltsbereich können inzwischen miteinander kommunizieren, sei es der Rasenmäher im Garten, die Jalousien am Fenster oder die Heizungsanlage im Keller. Sie alle können zudem zentral von der Nutzerin oder dem Nutzer, beispielsweise über eine App auf dem Smartphone, gesteuert werden. Es scheint praktisch und effizient, wenn die Heizung erst dann richtig aufdreht, wenn die Bewohner nach Hause kommen, oder der Rasenmäher vom Urlaubsort bedient werden kann. Auch die Möglichkeit, das Haustier zu Hause über angebrachte Kameras zu beobachten, wird von einigen geschätzt.

Ungleich umfassender sind die Vorstellungen zu den sogenannten Smart Cities, der Vernetzung und Interaktion von städtischen Bereichen wie beispielsweise dem Verkehr, der Infrastruktur, der Elektrizität und der Wasserversorgung oder der Abfallentsorgung. Auch hier sind viele hilfreiche Anwendungen denkbar, etwa das Dirigieren des Autos zum nächsten freien Parkplatz oder die Meldung des städtischen Mülleimers, dass er von der Stadtreinigung geleert werden muss.

Letzten Endes aber haben alle smarten Gegenstände eines gemeinsam: Sie sammeln Daten. Daten über sich, die Umgebung und über den Menschen. Und diese Daten sind in der Regel recht vielfältig, denn die meisten IoT-Geräte sind nicht gerade für ihre Datensparsamkeit bekannt.

Entgegen dem in der Europäischen Datenschutz-Grundverordnung (DS-GVO) verankerten Prinzip der Datenminimierung, vgl. Art. 5 Abs. 1 c, agieren die Geräte eher nach dem Motto „lieber zu viel als zu wenig“, schließlich könnten sich noch andere Verarbeitungszwecke ergeben. Entsprechend intransparent sind auch die meisten Datenschutzbestimmungen der Produkte und der dazugehörigen Apps gestaltet.

Was die smarten Geräte ebenfalls gemeinsam haben, ist deren „Kommunikationsfreudigkeit“, denn sie alle sind mit dem Internet verbunden und verfügen somit prinzipiell über die Fähigkeit, die Daten an Hersteller und an Dritte zu verschicken. Und davon machen die meisten auch rege Gebrauch. Daten sind im Zeitalter der Digitalisierung wertvoll, insbesondere personenbezogene Daten. Solche Daten - etwa die der Wearables - können vieles über die Nutzerin oder den Nutzer aussagen, zum Beispiel über Gewohnheiten, den Gemüts- oder Gesundheitszustand, wann man ins Bett geht oder aufsteht, wann man die Wohnung verlässt und wohin man geht. Damit lässt sich ein ziemlich umfassendes Profil über die Nutzerin oder den Nutzer bilden, siehe hierzu auch Zwölfter Tätigkeitsbericht, Punkt 4.1.3. Die Begehrlichkeiten bei Dritten werden in zunehmendem Maße geweckt. So bieten Krankenkassen bereits Tarife an, die einen Bonus versprechen, wenn sich Kundinnen oder Kunden gesundheitsbewusst verhalten. Autoversicherer bieten inzwischen Tarife an, die vom Fahrverhalten abhängen. Was für den einen gut ist, muss aber nicht für jeden gelten, denn die Gefahr von Diskriminierungen und Stigmatisierungen steigt kontinuierlich, besonders dann, wenn sich eine Nutzerin oder ein Nutzer der Offenlegung der Daten zu entziehen versucht oder schlicht nicht mehr in ein vorgesehenes Raster passt. Solch eine Entwicklung führt zwangsläufig zu einer entsolidarisierten Gesellschaft, in der genau diejenigen mit teuren Tarifen bestraft werden, die sich nicht „normgerecht“ verhalten oder aber einfach nur schlechte Werte liefern.

Mit Blick auf die kommende Datenschutz-Grundverordnung und die darin enthaltenen Grundsätze „Data Protection by Design“ und „Data Protection by Default“ werden Hersteller bei neuen Anwendungen jedoch umdenken müssen. Denn künftig dürfen auf den Geräten und den dazugehörigen Anwendungen nur noch so wenige Daten wie nötig erfasst und verarbeitet werden, zudem müssen die Voreinstellungen so datenschutzfreundlich wie möglich ausfallen. Das bedeutet, dass auch nur die Daten erfasst und verarbeitet werden dürfen, die für den jeweilig angedachten Zweck auch wirklich erforderlich sind. Dies betrifft neben der Dauer ihrer Speicherung, die so kurz wie nötig ausfallen muss, auch deren Zugänglichkeit. Es dürfen nur so viele wie wirklich nötig auf die Daten zugreifen.

Neben der Problematik der zügellosen Datensammelei muss in vielen Fällen auch die Datensicherheit kritisch betrachtet werden. So sollen die Geräte möglichst preiswert und nach möglichst kurzer Entwicklungszeit auf dem Markt angeboten werden. Eine angemessene Informationssicherheit etwa durch technische Schutzmaßnahmen oder gar Tests auf Schwachstellen mit dem Ziel einer späteren Nachbesserung, sofern neue Bedrohungen im Gerät entdeckt werden, bleiben dabei oft auf der Strecke. Entsprechend geben die Geräte, die als portable Mini-Computer angesehen werden müssen, ein attraktives Ziel für Hacker ab. Durch ihre Schwachstellen und angesichts der Tatsache, dass diese oftmals nur unzureichend oder gar nicht behoben werden, dienen diese Geräte vielfach als Basis für sogenannte Botnetze. Diese Botnetze, ein Zusammenschluss von kompromittierten Geräten, die ein Angreifer aus der Ferne kontrollieren kann, dienen dann als Ausgangspunkt für Angriffe auf Dritte.

Auf diese Weise können beispielsweise zeitgleich Daten oder Anfragen an bestimmte Webseiten oder Server geleitet werden, damit diese dann unter der Last zusammenbrechen. Derartige Angriffe sind bekannt als verteilte (engl. distributed) Denial of Service (DDoS) Attacken.

Wir empfehlen daher, sich genau zu überlegen, welche IoT-Geräte die Anschaffung wert sind, und zu prüfen, ob sowohl die Einstellungen als auch die Produktsicherheit den eigenen Vorstellungen entsprechen. Gefordert sind aber auch die Hersteller der Geräte, die verschärften Grundsätze der DS-GVO insbesondere zur Datenminimierung und zu den Grundsätzen „Data Protection by Design“ und „Data Protection by Default“ einzuhalten. Wir fordern die Hersteller daher auf, bereits bei der Projektplanung und -entwicklung die datenschutzrechtlichen Vorgaben zu berücksichtigen und einen nachhaltigen Produktzyklus zu etablieren, der das Erkennen und Schließen von Sicherheitslücken gewährleistet.

5.1.4 Infrastrukturenkomponenten nicht vergessen

Bei Kontrollen und Petitionsverfahren wurden wir mit der Frage konfrontiert, inwieweit technische Infrastrukturkomponenten in die datenschutzgerechte Gestaltung von Informationssystemen einbezogen werden müssen.

Hierbei ging es insbesondere um Virtualisierungslösungen wie VMWare und Citrix XenApp. Mithilfe solcher Lösungen werden Hardware- oder Softwareobjekte so nachgebildet, dass IT-Systeme in virtualisierten Umgebungen in derselben Weise ablaufen können wie auf echter Hardware oder echten Betriebssystemen. So können beispielsweise mehrere virtualisierte Server mit unterschiedlichen Betriebssystemen auf ein und demselben Computer laufen oder Plattenspeicher mehrerer Server können in einem einzigen Speichersystem zusammengefasst werden. Virtualisierungslösungen bieten oft auch zusätzliche Ausfallsicherheit, beispielsweise indem virtualisierte Server bei Defekt des Gerätes, auf dem sie laufen, automatisch auf ein anderes Gerät verschoben werden.

Virtualisierung kann - richtig eingesetzt - zu einer Verbesserung von technischem Datenschutz und Informationssicherheit beitragen. So kann die Fehlerrate bei der Administration gesenkt werden oder einheitliche Sicherheitsstandards auf einer Vielzahl gleichartiger virtueller Maschinen einfacher durchgesetzt werden. Anwendungen können besser gegen die Auswirkungen von Sicherheitslücken in anderen Anwendungen abgesichert werden, indem sie auf unterschiedlichen virtuellen Maschinen platziert werden.

Allerdings ist Virtualisierung kein informationstechnisches Allheilmittel. So ist Isolation unterschiedlicher virtueller Maschinen untereinander nicht perfekt und die Administratoren der Verwaltungssysteme haben grundsätzlich die Möglichkeit, sich Zugriff auf die laufenden virtuellen Maschinen zu verschaffen. Deshalb ist die Schutzwirkung einer Festplattenverschlüsselung beispielsweise in einer virtualisierten Umgebung geringer als auf echter Hardware. Das Bundesamt für Sicherheit in der Informationstechnik (*BSI*) führt im aktuellen Grundschutz-Kompendium insgesamt sieben spezifische Bedrohungstypen im Bereich Virtualisierung auf. Speichersystemen widmet das *BSI* ein zusätzliches Kapitel.

Verantwortliche müssen bei der Auswahl, Prüfung und Dokumentation von technischen und organisatorischen Datenschutzmaßnahmen jeweils alle Komponenten und Systeme betrachten, von denen potenziell Gefahren für die Verarbeitung personenbezogener Daten ausgehen können. Infrastrukturkomponenten, wie Virtualisierungssysteme und Speicherlösungen bilden keine Ausnahme. Weil moderne technische Infrastrukturkomponenten oftmals auf neuen Technologien basieren oder der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten dienen können, ist künftig auch zu prüfen, ob sie in eine Datenschutzfolgenabschätzung nach Art. 35 *DS-GVO* einzubeziehen sind.

Diese Erwägungen werden wir auch künftig unseren Beratungen und Kontrollen zugrunde legen.

5.1.5 elektronische Akte (eAkte)

Mit dem „Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern“, E-Government-Gesetz Mecklenburg-Vorpommern - EGovG M-V vom 25. April 2016, siehe dazu auch Zwölfter Tätigkeitsbericht, Punkt 5.4.1, will die Landesregierung die rechtlichen Rahmenbedingungen in der öffentlichen Verwaltung an die fortschreitende Digitalisierung der Gesellschaft anpassen. Auch Verwaltungstätigkeiten sollen künftig vollständig elektronisch und effizienter durchgeführt werden können.

Das neue Gesetz verpflichtet alle Behörden, ab dem 1. Januar 2020 ihre Akten elektronisch zu führen, soweit nicht wichtige Gründe entgegenstehen, siehe Art. 10 Abs. 1. Die Grundsätze ordnungsgemäßer Aktenführung sind dabei durch geeignete technische und organisatorische Maßnahmen nach dem Stand der Technik sicherzustellen.

Die ersten Erfahrungen im Umgang mit elektronischen Akten gibt es in der Landesregierung bereits, seitdem das Kabinett in seiner Sitzung am 29. April 2008 beschlossen hat, das elektronische Dokumentenmanagement- und Vorgangsbearbeitungssystem DOMEA ® in den Ministerien und der Staatskanzlei einzuführen. Seit dieser Zeit beraten wir die Landesregierung bei der Einführung und dessen Weiterentwicklung, siehe dazu auch Zehnter Tätigkeitsbericht, Punkt 4.3.2.

Mittlerweile ist das Support-Ende für DOMEA ® angekündigt, was zur Folge hat, dass auch eine technische Weiterentwicklung der Anwendung nicht mehr möglich ist. Eine solche Weiterentwicklung ist bei Softwareprodukten jedoch unabdingbar. Einerseits muss die Kompatibilität zu weiterer Software stets gewährleistet werden, insbesondere zum Betriebssystem und zu diversen Textbearbeitungssystemen. Andererseits müssen Sicherheitslücken und Programmfehler kontinuierlich durch sogenannte Patches geschlossen werden.

Um ein geeignetes Nachfolgeprodukt zu finden, ist zuerst ein Anforderungskatalog notwendig, welcher die wesentlichen Bedarfe der künftigen Nutzerinnen und Nutzer berücksichtigt. Der Anforderungskatalog wird zurzeit unter der Federführung des Ministeriums für Energie, Infrastruktur und Digitalisierung im Referat KeA, Kompetenzstelle elektronische Akte, erstellt. Mit einem umfassenden eAkte-System sollen auch zahlreiche personenbezogene Daten verarbeitet werden.

Deshalb ist eine Vielzahl von datenschutzrechtlichen Anforderungen zu berücksichtigen. Da das neue Verfahren sicher erst nach dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 in Betrieb gehen wird, müssen sich diese Anforderungen an der neuen Rechtsetzung orientieren. Folgerichtig ist deshalb neben den Vertretern aller Ressorts auch unsere Behörde in den Planungsprozess eingebunden.

Da beim geplanten Dokumentenmanagementsystem die Akten ausschließlich elektronisch gespeichert werden, sind neben den klassischen Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität, die sich aus Art. 32 DS-GVO zur Gewährleistung der Sicherheit der Verarbeitung ergeben, auch Fragen der Sicherstellung der Betroffenenrechte gemäß Art. 12, 13, 14 DS-GVO zur Wahrung der Transparenz, Zweckbindung und Intervenierbarkeit zu berücksichtigen. Das betrifft unter anderem Anforderungen an eine nachvollziehbare und transparente Verarbeitung des Verfahrens in Form von Protokollierungen. Protokollierung ist erforderlich, um nachvollziehen zu können, ob die personenbezogenen Daten rechtmäßig verarbeitet wurden. Es muss nachweisbar sein, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet, gelöscht oder übermittelt hat. Weiterhin muss mit Hilfe der Protokollierung nachweisbar sein, dass nur berechtigte Personen Änderungen am Dokumentenmanagementsystem durchgeführt haben. Fälschlicherweise wird diese Protokollierung der meist administrativen Tätigkeiten oft als Kontrolle der Tätigkeiten von Administratoren angesehen, jedoch dient dies vielmehr auch der Abwehr von unberechtigten Vorwürfen hinsichtlich eines Missbrauches ihrer administrativen Rechte.

Aus Gründen der Wirtschaftlichkeit ist nachvollziehbar, dass das neue Dokumentenmanagementsystem von mehreren Ministerien und Behörden gemeinsam genutzt werden soll. In diesem Fall müssen diese als eigenständige Mandanten im System agieren, damit eine Trennung der Daten und somit auch die Zweckbindung gewährleistet werden kann. Doch auch bei einer solchen Mandantentrennung ist eine Vielzahl von datenschutzrechtlichen Anforderungen zu berücksichtigen, denn eine gemeinsame Nutzung einer solchen Infrastruktur unterliegt erhöhten Anforderungen an die Trennung der personenbezogenen Daten, um die aus der gemeinsamen Nutzung entstehenden Risiken für die informationelle Gewaltenteilung, die Zweckbindung und Vertraulichkeit hinreichend zu reduzieren. In den Orientierungshilfen „Datenschutz bei Dokumentenmanagementsystemen“ [18] und „Mandantenfähigkeit“[19] haben die Datenschutzbeauftragten von Bund und Ländern zahlreiche Hinweise zur datenschutzgerechten Ausgestaltung dieser Systeme gegeben. Diese Orientierungshilfen sollten frühzeitig bei den Planungen des neuen eAkte-Systems herangezogen werden, auch um den Anforderungen der DS-GVO an Datenschutz durch Technikgestaltung, vgl. Art. 25 Abs. 1, gerecht zu werden.

[18] https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/oh_dms.pdf
[19] https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/oh_mandant.pdf

Der Begriff „Mandant“ oder „Mandantenfähigkeit“ wird häufig verwendet, wenn es Unternehmen, Behörden oder Organisationen ermöglicht werden soll, Daten in einer Datenbank logisch zu trennen und zu verwalten. Mit Hilfe der Mandantenfähigkeit können zum Beispiel Daten verschiedener Abteilungen einer Organisation/eines Unternehmens oder verschiedener Kunden eines IT-Services/Rechenzentrums getrennt vorgehalten werden.

5.1.6 Algorithmen

Die digitale Informationsgesellschaft entwickelt sich rasant. Sie ist geprägt von Verfahren, die in unterschiedlichster Art und Weise automatisierte Entscheidungen treffen. Hierbei bedienen sich die Verfahren unterschiedlichster Datenquellen, häufig bezeichnet als Big Data. Derartige Daten fallen bei der täglichen Nutzung von digitalen Geräten und Diensten in schier unerschöpflichen und scheinbar nicht auswertbaren Mengen an und können umfassend ausgewertet werden. Auf der Basis dieser Daten werden Entscheidungen inzwischen oft automatisiert getroffen, berechnet von Algorithmen. Sie prägen in steigender Anzahl den Alltag von Bürgerinnen und Bürger, ohne dass diese die Hintergründe kennen.

Ein Algorithmus an sich ist eine eindeutig festgelegte Handlungsanweisung, er beschreibt schrittweise, wie ein Problem durch logische Regeln gelöst werden kann. So begleiten uns die Algorithmen im täglichen Leben, angefangen bei den einfachsten Dingen, zum Beispiel dem Binden der Schuhe in erlernten Schritten, bis hin zu komplexen Berechnungen wie dem verkehrsabhängig optimalen Weg zum Urlaubsort. Algorithmen versprechen der Nutzerin oder dem Nutzer bei Internetrecherchen nur die Informationen, die (vermeintlich) auch wirklich benötigt werden, sie beantworten, eingebaut in modernste Smartphones und Lautsprecher, der Nutzerin oder dem Nutzer die Fragen und verwalten die Termine und damit auch den Tagesablauf. Auf den ersten Blick erspart diese zunehmende Algorithmisierung scheinbar viel Zeit und vereinfacht das Leben.

Doch gibt es auch eine Kehrseite der Medaille, beispielsweise dann, wenn nur noch Algorithmen entscheiden, ob man einen Kredit erhält oder welcher Versicherungstarif vermeintlich am besten zu einem passt. Algorithmen arbeiten dabei meist nach dem Prinzip einer Blackbox. Welche Daten als Grundlage für die Angebote herangezogen werden und wie diese zur Entscheidungsfindung dienen, ist in vielen Fällen weder den Betroffenen und oftmals noch nicht einmal mehr dem Anbieter selbst ersichtlich. Versprochen wird Neutralität und Objektivität, basierend auf mathematisch-statistischen Berechnungen von Wahrscheinlichkeiten. Die individuelle Situation von Betroffenen kann der Algorithmus dabei jedoch nicht berücksichtigen. Es besteht die Gefahr von Diskriminierungen und Stigmatisierungen, eingeschränkten Auswahlmöglichkeiten sowie von einzelnen Fehlentscheidungen.

Diese Fehler werden oft als vernachlässigbare Nebenwirkungen einer schnellen und vermeintlich nachhaltigen Informationsgesellschaft angesehen. Sie sind aber von den Verantwortlichen einkalkuliert und müssen von den Betroffenen akzeptiert werden. Vergessen werden darf aber nicht, dass Algorithmen von Programmierern und Entwicklern entworfen und umgesetzt werden und dass die Algorithmen damit auch nach deren Werturteilen handeln.

Doch selbst, wenn die Werturteile richtig scheinen, sind auch Experten nur Menschen, denen Fehler unterlaufen können, Fehler oder Werturteile, die in der Folge schnell auch einmal den Falschen treffen können. Die Falschen trifft es auch dann, wenn diese versuchen, nicht aufzufallen, ein dem Algorithmus entsprechendes und vermeintlich konformes Verhalten an den Tag zu legen. Doch ein kontinuierliches Mitschwimmen in einer breiten Masse, möglichst ohne auffällige Schwankungen, die sonst den Kredit verwehren oder die Versicherungen teuer werden lassen würden, hat nichts mit einem selbstbestimmten Leben zu tun.

Entsprechend wichtig ist es, dass Transparenz und Nachvollziehbarkeit beim Einsatz von Algorithmen vorherrschen. Bürgerinnen und Bürger haben ein Recht darauf zu erfahren, wenn Entscheidungen über sie auf automatisierten Einzelentscheidungen beruhen und auf welchen zugrundeliegenden Daten und Bewertungskriterien diese fußen. Hierzu gehört, dass den Betroffenen das Recht eingeräumt werden muss, automatisierte Einzelentscheidungen von einer unabhängigen Aufsichtsbehörde überprüfen und, falls erforderlich, revidieren lassen zu können. Die Anwendung von Algorithmen darf auch nicht zu einem Unterhöhlen des Datensparsamkeitsprinzips führen.

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.

5.2 Kommunikation/neue Medien

5.2.1 TLSA/DANE - Internetdienste besser sichern

Ein Petent beschwerte sich über die Informationssicherheit des Verfahrens IDEV (Internet-Datenerhebung im Verbund). Mit diesem Verfahren erhebt das Statistische Amt Mecklenburg-Vorpommern Daten für den Mikrozensus (siehe Zwölfter Tätigkeitsbericht, Punkt 5.8.2). Der Petent rügte unter anderem, dass das Verfahren nicht die Sicherungsmechanismen TLSA/DANE nutzt.

TLSA/DANE unterstützt TLS (Transport Layer Security), das bekannte Protokoll zur sicheren Übertragung von Daten im Internet (ebenda). Damit eine Person oder ein Programm sicher sein kann, mit welchem Server sie kommunizieren, benötigen sie ein Zertifikat des Servers. Dieses Zertifikat wird üblicher Weise von besonderen Organisationen, den Zertifizierungsstellen, ausgestellt.

Zertifizierungsstellen können grundsätzlich für beliebige Adressen von Servern Zertifikate ausstellen. Eine fehlerhaft arbeitende Zertifizierungsstelle genügt folglich, um das Vertrauen in diese Infrastruktur zu erschüttern. Manche Zertifizierungsstellen haben in der Vergangenheit gravierende Fehler bei der Ausstellung von Zertifikaten gemacht. Zertifikate lauteten auf Adressen von Servern, die sich nicht unter der Kontrolle des Antragstellers befanden. Mithilfe solcher gefälschter Zertifikate können Unbefugte Kommunikationsinhalte, die nicht für sie bestimmt sind, abhören. Bekannt geworden ist insbesondere der Fall der Zertifizierungsstelle Diginotar (siehe Zehnter Tätigkeitsbericht, Punkt 4.2.6).

Nutzerinnen und Nutzer können dem teilweise entgegenwirken, indem sie die Zertifikate auf Plausibilität prüfen. In Webbrowsern kann man sich hierzu Informationen über die gerade verwendeten Zertifikate anzeigen lassen, indem man auf das Schlosssymbol neben dem Adressfeld klickt.

Einfacher und für Nutzerinnen und Nutzer bequemer ist es, den Serverbetreibern mehr Kontrolle über die verwendeten Zertifikate zu geben. Dies leistet TLSA/DANE, indem es Zertifikate über die gesicherte Variante des Domain Name Systems (DNS), nämlich DNSSEC verteilt. Mit dem DNS werden unter anderem sprechende Namen wie www.datenschutz-mv.de in aus schlecht zu merkenden Zahlen bestehende IP-Adressen umgesetzt, die benötigt werden, um im Internet Verbindungen herstellen zu können. DNSSEC sorgt für eine sichere Verteilung dieser Daten, denn die DNS-Einträge sind hier digital signiert. Auf Seiten des Nutzers kann spezielle Software dann prüfen, ob das von einem Webserver, Mailserver oder einem anderen Internetdienst bereitgestellte Zertifikat über DNSSEC bezogen wurde.

Webbrowser unterstützen dieses Verfahren bislang praktisch nicht. Jedoch ist hier der praktische Nutzen auch nicht so hoch wie in anderen Einsatzszenarien, denn Nutzerinnen und Nutzer können, wie beschrieben, die ihnen von Webservern präsentierten TLS-Zertifikate selbst prüfen. Ein TLSA/DANE-fähiger Browser könnte zusätzlich anzeigen, ob die Verbindung auch mit diesem Verfahren gesichert ist. Es wäre möglich, Verbindungen abzuweisen, für die dies nicht gilt. Wegen der geringen Marktdurchdringung des Verfahrens wäre dies jedoch nicht anzuraten, da sehr viele Websites durch diese Prüfung fallen würden.

Interessanter ist der Einsatz von TLSA/DANE derzeit bei vollständig automatisierten Kommunikationen im Internet, beispielsweise bei der Übertragung von E-Mails. Mail-Server, die Mails mit TLS-verschlüsselten Verbindungen austauschen, sind derzeit Stand der Technik. Etliche große Provider setzen diese Technik bereits ein. Wird hier TLSA/DANE zusätzlich genutzt, so können Mail-Server automatisiert prüfen, ob eingehende verschlüsselte Verbindungen aus zuverlässigen Quellen stammen.

Deshalb raten wir dazu, bereits heute TLSA/DANE zur Sicherung der E-Mail-Kommunikation und vergleichbarer Protokolle einzusetzen. Für Webserver halten wir dies bisher nur mittelfristig für angezeigt. Abzuwarten bleibt, wie sich die Unterstützung dieses Verfahrens in Webbrowsern entwickeln wird. Wir haben gegenüber dem Statistischen Amt deshalb nicht auf einer Implementation dieser Technik im Rahmen des Verfahrens IDEV bestanden.

5.2.2 Neugestaltung des „Virtuellen Datenschutzbüros“

Als „Virtuelles Datenschutzbüro“ wird die gemeinsame Webseite[20] verschiedener Projektpartner aus dem Bereich des Datenschutzes bezeichnet. Zu den Projektpartnern gehören dabei alle unabhängigen Datenschutzbehörden des Bundes und der Länder und Vertreter der Datenschutzbeauftragten von Kirchen und Rundfunkanstalten. Hinzu kommen noch Datenschutzbeauftragte aus den Ländern Schweiz, Liechtenstein und Polen. Das Informationsangebot dieser Seite richtet sich in erster Linie an die Bürgerinnen und Bürger.

[20] https://www.datenschutz.de

Die Webseite verfolgt das Ziel, den Besucherinnen und Besuchern einen zentralen Einstiegspunkt für Informationen zum Thema Datenschutz anzubieten. Neben grundlegenden rechtlichen Informationen erhalten sie auch einen Überblick, an welche Aufsichtsbehörde sie sich im konkreten Fall wenden können. Die Besucher finden zudem erste praktische Informationen und Hinweise, wie sie sich selbst sicher im Internet bewegen können. Darüber hinaus bündelt die Webseite zahlreiche News zu aktuellen datenschutzrechtlichen Veröffentlichungen aller Projektpartner.

Um mit den technologischen Entwicklungen sowie den fortschreitenden Angeboten im Internet Schritt zu halten, ist eine kontinuierliche Entwicklung der Webseite notwendig. Mit Blick auf die stetig steigenden Nutzerzahlen von mobilen Endgeräten, wie Tablets oder Smartphones, zählt hierzu insbesondere auch die Ausrichtung des Webseitendesigns auf die kleineren Displaygrößen.

Wir haben uns an der Projektgruppe, welche die Neugestaltung und Neuausrichtung der Webseite im April 2016 abgeschlossen hat, maßgeblich beteiligt. Der Mehrwert für die Besucherinnen und Besucher dieser zentralen Seite, die neben umfangreichen News und Hinweisen auch eine Suche über alle Webseiten der beteiligten Partner hinweg ermöglicht, ist aus unserer Sicht sehr groß. Das „Virtuelle Datenschutzbüro“ hat sich über Jahre hinweg einen bekannten Namen erarbeitet und dient damit vielen Bürgerinnen und Bürgern als erste Anlaufstelle bei datenschutzrechtlichen Fragestellungen und Problemen. Wir werden uns auch weiterhin aktiv an den Arbeiten zur Gewährleistung der Aktualität des „Virtuellen Datenschutzbüros“ beteiligen.

5.3 Videoüberwachung

5.3.1 Einsatz einer Rettungsdrohne durch das DRK

Von Beginn an und in sehr guter Zusammenarbeit mit dem DRK-Kreisverband Ostvorpommern-Greifswald haben wir dessen Projekt zum Einsatz eines Multicopters (umgangssprachlich „Drohne“) zur Unterstützung der Rettungsschwimmer aus der Luft datenschutzrechtlich begleitet.

Rettungsschwimmer haben es an überfüllten Stränden schwer, schnell zu den Hilfesuchenden durchzudringen. In einem Notfall startet deshalb der Rettungscopter (parallel zum Rettungsschwimmer), fliegt auf schnellstem Wege zum Hilfesuchenden und wirft eine Schwimmhilfe ab, die sich bei Wasserkontakt entfaltet. Diese liefert einen ersten Halt, bis der Rettungsschwimmer auf dem herkömmlichen Weg eintrifft - wertvolle Zeit, die am Ende über Leben und Tod entscheiden kann. Außerdem soll der Copter im Falle einer Vermisstenanzeige das vermutete Wasserareal aus der Luft erkunden, um die vermisste Person aufgrund der besseren Übersicht schneller retten zu können.

Organisationen mit Sicherheitsaufgaben, zu denen auch das DRK zählt, haben nach § 21 a Absatz 2 Nr. 2 Luftverkehrsordnung einen Sonderstatus, der es ihnen gestattet, unbemannte Flugsysteme wie Copter in sensiblen Bereichen, wie bei Unfällen und über Menschenansammlungen, zu nutzen.

Unabhängig davon hat der DRK-Kreisverband Ostvorpommern-Greifswald die potenziell datenschutzkritischen Aspekte bei Drohnen-Flügen über Badestränden von Anfang an aufmerksam im Blick gehabt und im Projekt stets großen Wert auf entsprechende Maßnahmen zur Gewährleistung des Datenschutzes gelegt.

So wurde der Einsatz des Copters strikt auf den Abwurf der Schwimmhilfe, die Suche nach Vermissten und das Training begrenzt. Über den tatsächlichen Einsatz entscheidet ausschließlich der Wachleiter.

Ferner erfolgt der Flug über den Strand mit nach vorn (und nicht nach unten) ausgerichteter Kamera. Erst über dem Wasser wird diese nach unten gerichtet, um den Hilfesuchenden schnell zu finden und die Schwimmhilfe exakt abzuwerfen.

Dabei sieht der „Pilot“ die Live-Bilder auf seinem Empfangsgerät, es findet jedoch keine Aufzeichnung des Einsatzgeschehens und keine Beobachtung des Strandes statt.

Alle „Piloten“ werden umfassend im Datenschutz unterwiesen und auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetz verpflichtet. Verbote gelten insbesondere für: Fliegen ohne Notsituation, Steuerung durch nicht geschultes Personal und für die Zweckentfremdung der Technik, z. B. Beobachtung von Strandbesuchern zum Spaß, bzw. Aufnahme von Bildern, die Rückschluss auf Einzelpersonen ermöglichen und diese deutlich erkennbar machen.

Hinweise und Informationen über mögliche Flüge des Rettungscopters erfolgen umfassend durch Hinweisschilder an den Strandzugängen, eine Copter-Flagge am Rettungsturm, Presseinformationen und Medienberichte, sowie durch Informationsflyer bei den Rettungsschwimmern am Strand, bei den Kurverwaltungen und Gastgebern - jeweils mit allen Informationen und dem Link zu einer eigenen Projekt-Info-Website des DRK-Kreisverbands Ostvorpommern-Greifswald e. V.

5.3.2 Einsatz von Drohnen durch eine Freiwillige Feuerwehr

Eine Freiwillige Feuerwehr hat bei uns angefragt, ob bei Feuerwehreinsätzen dem Einsatz von Drohnen aus datenschutzrechtlicher Sicht etwas entgegensteht. Unter anderem sollten die mit der Drohne gewonnenen Videosequenzen gespeichert werden.

Zunehmend werden für verschiedene Zwecke Drohnen genutzt. Mit einem Einsatz von Drohnen geht sowohl die Gefahr von Kollisionen, Abstürzen oder Unfällen als auch die Beeinträchtigung der Privatsphäre durch missbräuchliche Nutzung einher. Um dies rechtlich zu ordnen, wurde im März 2017 die Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten erlassen, durch die wiederum auch die Luftverkehrs-Zulassungs-Ordnung (*LuftVZO*) geändert wurde. Nach § 21a Abs. 1 LuftVZO ist der Betrieb von Drohnen genehmigungspflichtig, wenn diese beispielsweise mehr als 5 Kilogramm Startmasse haben. Unabhängig hiervon darf mit Drohnen grundsätzlich auch nicht über Menschenansammlungen oder Wohngrundstücken geflogen werden (§ 21b LuftVZO).

Weder das Überflugverbot noch die Genehmigungspflicht gelten für Organisationen mit Sicherheitsaufgaben im Zusammenhang mit Not- und Unglücksfällen sowie Katastrophen. Hierunter fallen im Einsatzfall auch Freiwillige Feuerwehren.

Unter den vorgenannten Voraussetzungen wäre ein Einsatz von Drohnen somit zunächst einmal möglich. Unberücksichtigt darf jedoch nicht bleiben, dass die LuftVZO lediglich Regelungen zur Erlaubnis des Betriebes/der Benutzung von Drohnen trifft, datenschutzrechtliche Aspekte aber nicht betrachtet werden. Das für den Bereich Brandschutz anzuwendende Brandschutz- und Hilfeleistungsgesetz M-V (BrSchG) verweist in § 28 auf das Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V).

Eine Speicherung von Videosequenzen wäre nach § 11 Abs. 1 DSG M-V nur möglich, wenn dies für die Aufgabenerfüllung erforderlich ist. Diese Erforderlichkeit haben wir nicht gesehen. Vielmehr haben wir darauf hingewiesen, dass die Nutzung von Drohnen immer durch den jeweiligen Einsatz und die damit zusammenhängenden Notwendigkeiten gerechtfertigt sein muss und somit eher restriktiv erfolgen sollte. Des Weiteren dürfte ein Beobachten (Drohne mit Kamera als „verlängertes Auge“) ausreichen. Dieses Beobachten dürfte beispielsweise bei der Gewinnung von Übersichtsbildern im Brandfall oder auch bei Durchführung einer Brandwache hilfreich sein.

5.3.3 „Nachbarschaftliche“ Videoüberwachung

Videokameras werden durch den technischen Fortschritt, die damit einhergehende immer günstiger werdende Produktion und die Vielzahl der Anbieter für jedermann erschwinglich. Dies zeigt sich auch zunehmend im Rahmen von nachbarschaftlichen Streitigkeiten und Auseinandersetzungen, in welchen Videokameras als technisches Hilfsmittel - entweder zur Einschüchterung oder um sich gegen tatsächliche oder vermeintliche Angriffe des Nachbarn zu wehren und diese zu dokumentieren - genutzt werden.

Die Hintergründe der nachbarschaftlichen Auseinandersetzungen sowie die damit zusammenhängenden Aktionen und Reaktionen sind teilweise sehr skurril. So wurde beispielweise mitgeteilt, dass der Nachbar über den Zaun in den Garten uriniert, dass der Nachbar Müll in den Garten wirft, dass die aufgehängte Unterwäsche der Frau von der Wäscheleine gestohlen wurde, dass Giftköder für Hunde und Katzen ausgelegt wurden, aber auch, dass der Betroffene Opfer von Sachbeschädigung und Vandalismus durch Beschmierungen und Graffiti geworden ist. Als Gegenmaßnahme wird dann in vielen Fällen die Installation einer Videokamera gesehen. Die Installation von Videokameras ist in der Regel nicht die Ursache dieser nachbarschaftlichen Streitigkeiten. Die Kameras sind vielmehr ein weiteres Instrument im Rahmen der eskalierenden Auseinandersetzungen.

Bei der datenschutzrechtlichen Beurteilung ist zu berücksichtigen, dass die Videoüberwachung des eigenen privaten Grundstücks grundsätzlich möglich ist, solange kein öffentlich zugänglicher Raum oder Nachbargrundstücke überwacht werden. Die Videoüberwachung von öffentlich zugänglichem Raum unterliegt demgegenüber den Zulassungsvoraussetzungen des § 6 b Bundesdatenschutzgesetz (*BDSG alt*).

Im Gegensatz zur Überwachung des eigenen Grundstücks ist die Videoüberwachung öffentlich genutzten Straßenraums grundsätzlich unzulässig, wobei die Erfassung eines schmalen Streifens entlang der Hauswand unter bestimmten Umständen nach der Rechtsprechung ausnahmsweise zulässig sein kann.

In den Fällen, in denen öffentlich genutzter Straßenraum von der Kamera „mitüberwacht“ wird, ist entweder der Aufnahmebereich per Kameraeinstellung so zu ändern, dass dies nicht mehr der Fall ist, oder die Kamera ist zu deinstallieren.

Die Überwachung von Privatgrundstücken (auch dem des Nachbarn) unterfällt demgegenüber wegen der nichtöffentlichen Zugänglichkeit nicht dem § 6 b BDSG (alt). Das Bundesdatenschutzgesetz ist zwar gemäß § 1 Abs. 2 Nr. 3 BDSG (alt) nicht anwendbar, wenn die Datenverarbeitung zu persönlichen oder familiären Zwecken erfolgt. Gegen die Überwachung von Privatgrundstücken, zum Beispiel durch Nachbarn, bestehen allerdings für Betroffene in der Regel zivilrechtliche Unterlassungs- und Abwehransprüche nach den §§ 1004, 823 Bürgerliches Gesetzbuch (*BGB*). Diese Ansprüche müssen allerdings durch die Betroffenen selbst auf dem Zivilrechtsweg und gegebenenfalls unter Einschaltung eines Rechtsanwalts durchgesetzt werden.

5.3.4 Videoüberwachung in einem Jugendfreizeittreff

Ist Videoüberwachung tatsächlich ein geeignetes Mittel, um Vandalismus zu verhindern? Mit dieser Frage mussten wir uns im Berichtszeitraum einige Male befassen.

So plante unter anderem eine Kommune, in ihrem Jugendfreizeittreff eine Videoüberwachungsanlage zu installieren. Mit dieser sollten alle Räume und auch Außenbereiche überwacht werden, um möglichen Vandalismus-Schäden entgegenzuwirken.

Wenn es um Eigentums- bzw. Besitzschutz, also um die Frage des Hausrechts geht, kommt § 37 Landesdatenschutzgesetz (DSG M-V) als Ermächtigungsgrundlage in Betracht. Hiernach ist ein Beobachten mittels Videoüberwachung dann erlaubt, wenn dies zur Wahrnehmung des Hausrechts erforderlich ist und schutzwürdige Belange Betroffener nicht überwiegen.

Bei einer vor-Ort-Besichtigung stellten wir fest, dass in dem Jugendfreizeittreff bestimmte Räumlichkeiten bereits videoüberwacht wurden. Diese Videobilder dienten als „verlängertes Auge“ für die Mitarbeiterinnen und Mitarbeiter. Konkret waren die bereits im Einsatz befindlichen Kameras auf einen kleinen Bildschirm so aufgeschaltet, dass diese Bilder nur für Befugte sichtbar waren. Außerdem wurden durch die Kameras keine hochauflösenden Bilder gemacht. Dennoch konnte auf dem Bildschirm erkannt werden, in welchem Bereich des Treffs es zu möglichen kritischen Situationen, beispielsweise anbahnende Sachbeschädigungen oder Raufereien, kommen würde.

Da der Jugendfreizeittreff durch das breite Freizeitangebot über etliche Räumlichkeiten verfügte, war es den Mitarbeiterinnen und Mitarbeitern nicht möglich, zeitgleich überall zu sein. Um einen geordneten Ablauf innerhalb der Einrichtung gewährleisten zu können, machte es durchaus Sinn, sich einer Videoüberwachung mit beobachtender Funktion zu bedienen. Insofern war die bereits im Einsatz befindliche Videoüberwachung ein probates Hilfsmittel und entsprach auch den rechtlichen Bedingungen.

Eine darüber hinausgehende Videoüberwachung hielten wir unter Berücksichtigung der in § 37 DSG M-V enthaltenen Interessensabwägung für nicht erforderlich und haben daher die Empfehlung ausgesprochen, von der angedachten Modernisierung und Erweiterung der Videoüberwachungsanlage Abstand zu nehmen.

5.3.5 Videoüberwachung an Schulen

Vielerorts sind Graffiti-Schmierereien ein ernst zu nehmendes Problem. Hiervon sind vor allem auch Gebäude, die zu bestimmten Zeiten nicht oder nur wenig genutzt werden, betroffen, unter anderem auch Schulen. Um diesem Problem entgegenwirken zu können, planen einige Kommunen die Einrichtung von Videoüberwachungsanlagen.

Bei der Einrichtung von Videoüberwachungsanlagen muss jedoch bedacht werden, dass jede Videoüberwachung in das Recht der betroffenen Personen auf informationelle Selbstbestimmung eingreift. Insofern sollten derartige Vorhaben nicht unkritisch hingenommen werden. Ziel sollte vielmehr sein, einen Ausgleich zwischen den Eigentumsinteressen und den Persönlichkeitsrechten herzustellen.

Bei der datenschutzrechtlichen Bewertung eines uns vorliegenden Falles, wo an einer Schule Videoüberwachungsanlagen vorgesehen beziehungsweise bereits installiert waren, mussten wir uns mit der Frage befassen, ob es sich bei Schulhöfen um öffentlich zugängliche Räume handelt, da nur dann der Anwendungsbereich des § 37 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) gegeben wäre.

Der betreffende Schulträger war der Meinung, dass die öffentliche Zugänglichkeit nicht gegeben sei. Diese Auffassung teilten wir nicht. Vielmehr dürften Schulhöfe grundsätzlich zu den Bereichen gehören, die frei oder nach allgemein erfüllbaren Voraussetzungen betreten werden können. Grundsätzlich dürften Schulhöfe so gestaltet sein, dass sie auch außerhalb von Schulzeiten von Schülerinnen und Schülern, Lehrkräften oder Dritten genutzt werden. Bei Schülerinnen und Schülern könnte dies beispielsweise zur Freizeitgestaltung der Fall sein. Von daher sind Schulhöfe dem öffentlichen Bereich zuzurechnen und unterfallen damit dem gesetzlichen Anwendungsbereich des § 37 DSG M-V. Mit dem Schulträger konnte bislang noch kein Konsens zu diesem Punkt herbeigeführt werden, sodass wir uns noch nicht mit Detailfragen der Videoüberwachung befassen konnten.

Grundsätzlich darf eine Videoüberwachung mit Speicherung durchgeführt werden, wenn dies zur Abwendung einer konkreten Gefahr oder zu Zwecken der Beweissicherung erforderlich ist. Dem vorangestellt muss die generelle Erforderlichkeit der Videoüberwachung, also schon das Beobachten, und damit die Verhältnismäßigkeit geprüft werden. Dabei muss unter mehreren möglichen und geeigneten Maßnahmen diejenige getroffen werden, die den Einzelnen und die Allgemeinheit am wenigsten beeinträchtigt. Außerdem darf nicht unberücksichtigt bleiben, dass gerade im Schulbereich die Entwicklung der Schülerinnen und Schüler zu selbstbestimmten Persönlichkeiten im Fokus stehen sollte. Inwieweit dieser Auftrag mit einer Videoüberwachung in Einklang zu bringen ist, ist kritisch zu hinterfragen.
Sofern die gesetzlichen Voraussetzungen erfüllt sind, kann im Einzelfall eine Videoüberwachung durchgeführt werden. Dies könnte beispielsweise außerhalb der Schulbetriebszeiten der Fall sein.

6 Datenschutz in verschiedenen Rechtsgebieten

6.1 Rechtswesen

6.1.1 Verletzung der Auskunftspflicht kann teuer werden

Nach § 34 Abs. 1 Bundesdatenschutzgesetz (*BDSG alt*) besteht ein Auskunftsrecht über die zur eigenen Person gespeicherten Daten, zum Zweck der Speicherung, zu deren Herkunft und zur Weitergabe der personenbezogenen Daten. Nach § 28 Abs. 4 *BDSG* kann der Betroffene ferner eine Sperrung für Werbezwecke verlangen (Werbewiderspruch). Dies wird seitens der Unternehmen gelegentlich vernachlässigt, jedoch nach Intervention unsererseits nachgeholt und beachtet.

In einem Fall zeigte sich ein Geschäftsinhaber jedoch völlig uneinsichtig sowohl gegenüber den genannten Betroffenenrechten als auch gegenüber deren Durchsetzung durch unsere Behörde. Er teilte mit, generell keine Auskunft zu Kundendaten zu geben, äußerte sich in der Sache selbst überhaupt nicht und übersandte uns statt dessen eine „Rechnung“ über 50,00 Euro für seine Aufwendungen mit der Bitte um umgehende Begleichung.

Wir haben daraufhin einen Anordnungsbescheid erlassen, ein Zwangsgeld im oberen dreistelligen Bereich festgesetzt und (für den Fall der fortgesetzten Auskunftsverweigerung) ein zweites Zwangsgeld in doppelter Höhe angedroht.

Der Geschäftsinhaber hat daraufhin über seinen Anwalt Klage vor dem Verwaltungsgericht gegen unseren Bescheid erhoben - diese jedoch im weiteren Verlauf wieder zurückgenommen.

Der Anordnungs- und Zwangsgeldbescheid ist rechtskräftig und wird vollstreckt. Der Auskunftspflichtige kann die Zahlung des angedrohten zweiten Zwangsgeldes abwenden, indem er Auskunft erteilt und die an ihn gerichteten Fragen beantwortet. Tut er dies nicht, werden weitere Zwangsgelder festgesetzt und vollstreckt, bis die oben genannten Betroffenenrechte durchgesetzt sind.

6.1.2 Einscannen von Personalausweisen und Pässen bei Schiffsreisen

Im Rahmen einer Petition wurde uns mitgeteilt, dass ein Kreuzfahrtunternehmen beim Antritt der Reise die Personalausweise der Kunden einscannt.

Das Unternehmen erklärte, dass die maschinenlesbare Zone der Dokumente ausgelesen wird, um die Reisedokumente mit den vorhandenen Schiffsmanifestdaten abzugleichen und gegebenenfalls zu korrigieren. Nach diesem Abgleich werden die Daten aus dem Scan sofort gelöscht. Die maschinenlesbare Zone (Machine Readable Zone - MRZ) ist dafür angelegt, um sie mit einer optischen Texterkennung auslesen zu können. Sie enthält die Datensätze Vorname, Name, Geburtsdatum, Staatsangehörigkeit, Kennzahl der ausstellenden Behörde, Dokumentenart und Seriennummer sowie Datum der Gültigkeit des Dokuments. Diese Daten der Reisenden werden benötigt, um fremde Häfen während der Kreuzfahrt anlaufen zu können und diesbezüglich den internationalen Meldepflichten nachzukommen.

Nach § 20 Abs. 4 Personalausweisgesetz (*PAuswG*) und § 18 Abs. 4 Passgesetz (*PassG*) dürfen Beförderungsunternehmen personenbezogene Daten aus der maschinenlesbaren Zone des Personalausweises bzw. des Passes elektronisch nur auslesen und verarbeiten, soweit sie auf Grund internationaler Abkommen oder Einreisebestimmungen zur Mitwirkung an Kontrolltätigkeiten im internationalen Reiseverkehr und zur Übermittlung personenbezogener Daten verpflichtet sind. Biometrische Daten dürfen nicht ausgelesen werden.

In der Kommunikation mit dem Kreuzfahrtunternehmen stellte sich heraus, dass die verwendeten Lesegeräte an Bord der Schiffe ein Bild vom Ausweis oder Pass machen, aus welchem die integrierte optische Texterkennung dann die Daten aus der maschinenlesbaren Zone ausliest. Problematisch hierbei war, dass durch das vom Lesegerät gemachte Bild mehr personenbezogene Daten erhoben wurden, als erforderlich waren. Das waren beim neuen chipkartengroßen Personalausweis, bei dem sich die maschinenlesbare Zone auf der Rückseite befindet, die Augenfarbe, die Körpergröße, die Anschrift und das auf der Rückseite befindliche Laserkippbild.

Das Kreuzfahrtunternehmen nahm infolgedessen mit der Firma, die die Software für die Lesegeräte erstellt hatte, Kontakt auf und ließ die Software so umprogrammieren, dass nur noch die maschinenlesbare Zone der Dokumente aufgenommen wird, sodass nur noch die gesetzlich zulässigen Daten erhoben werden.

6.1.3 „Strafzettel“ auf privatem Parkplatz

Einige Petitionen im Berichtszeitraum bezogen sich auf die Datenerhebung im Rahmen des gelegentlich von Markt-/Einkaufszentren praktizierten Parkplatzmanagements, bei dem externe Firmen mit der Kontrolle der firmeneigenen Kundenparkplätze beauftragt werden.

Anlass war die Frage, ob diese beauftragten Firmen berechtigt sind, mit dem erhobenen Kennzeichen eine Halterabfrage beim Kraftfahrzeugbundesamt zu stellen, um danach eine Kostenforderung zu versenden. Anlass war jedoch ebenso die Höhe dieser Kosten, die meist deutlich über den Verwarngeldern lag, die im öffentlichen Verkehrsraum von den zuständigen kommunalen Ordnungsämtern festgesetzt werden.

Gemäß § 28 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben, Speichern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung oder Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist oder soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Indem der jeweilige Kunde sein Fahrzeug auf einem firmeneigenen Kundenparkplatz parkt, erklärt er sich mit den dort geltenden Nutzungsbedingungen einverstanden und schließt konkludent einen entsprechenden (Nutzungs-)Vertrag. Hierzu wird an der Zufahrt des Parkplatzes mit Hilfe von Schildern auf den Vertragspartner und auf die Nutzungsbedingungen aufmerksam gemacht. Im Rahmen dieser Regelung ist es auch möglich, Fotos von Fahrzeugen anzufertigen, um Verstöße zu dokumentieren.

Auch eine Halterabfrage beim Kraftfahrzeugbundesamt ist in der Regel nach § 39 Abs. 1 Straßenverkehrsgesetz (StVG) zulässig. Danach sind die Daten zu übermitteln, wenn der Empfänger (hier die jeweilige Firma) unter Angabe des betreffenden Kennzeichens darlegt, dass die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt werden.

Dabei genügt ein mittelbarer Zusammenhang mit der Teilnahme am Straßenverkehr. Dies ist insbesondere dann der Fall, wenn das Kraftfahrzeug in Gebrauch ist. Eine Teilnahme am Straßenverkehr kann aber auch vorliegen, wenn das Kraftfahrzeug abgestellt ist. Der Gebrauch des Kraftfahrzeuges muss sich dabei nicht unbedingt im öffentlichen Straßenverkehr abspielen. Es genügt, wenn das Fahrzeug auf einem privaten Parkplatz abgestellt ist.

Bei der Beurteilung der Rechtmäßigkeit der Kostenforderung und deren Höhe im jeweiligen Einzelfall handelt es sich nicht um eine datenschutzrechtliche Fragestellung, sondern um eine Frage, die gegebenenfalls im Wege eines Zivilprozesses vor dem Amtsgericht zu klären ist.

6.2 Polizei/Ordnungswesen

6.2.1 Bodycams bei der Polizei in Mecklenburg-Vorpommern

Die Landesregierung hat ein Gesetz zur Änderung des SOG auf den Weg gebracht, damit zukünftig 45 ausgewählte Polizeibeamtinnen und -beamte Schulterkameras nebst kleinen Bildschirmen auf der Brust tragen können. Die sogenannten Bodycams sollen polizeiliche Einsätze mit Bild und Ton aufzeichnen.

Rechtsgrundlage für die Erprobung der Bodycams soll der neu einzufügenden § 32a SOG M-V sein. Zum Schutz der Polizeibeamtinnen und -beamten können Personen in Bild- und Ton aufgenommen werden, die im Rahmen der Gefahrenabwehr und bei der Verfolgung von Straftaten oder OWI im öffentlichen und privaten Raum angetroffen werden. Gegen eine damit einhergehende Ausweitung der Videoüberwachung durch die Polizei haben wir im Gesetzgebungsverfahren Bedenken geäußert. In unserer Stellungnahme zu dem Gesetzentwurf haben wir darauf hingewiesen, dass der Einsatz von Bodycams im öffentlichen und im privaten Bereich typischerweise mit Eingriffen in das Recht auf informationelle Selbstbestimmung als besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art 1 Abs 1 GG) sowie ggf. in das Recht auf Unverletzlichkeit der Wohnung eingegriffen wird. Die Ermächtigungsgrundlage, der es für den Einsatz von Bodycams bedarf, muss den Anlass, den Zweck und die Grenzen des Eingriffs bereichsspezifisch, präzise und normenklar festlegen. Diese Ermächtigungsgrundlage soll mit § 32a SOG M-V geschaffen werden, und wir haben im Gesetzgebungsverfahren die Möglichkeit des sogenannten Pre-Recording kritisch hinterfragt. Bei Einschaltung dieser Funktion werden in einem erweiterten Standby-Betrieb Bild und Ton auch ohne individuelle Aktivierung der Aufnahme durch den kameraführenden Beamten für einen Zeitraum von 60 Sekunden fortlaufend in einer Aufzeichnungsschleife aufgenommen. Erfolgt keine Aktivierung der eigentlichen Kameraaufzeichnung, so werden die Daten zwar nach Ablauf der eingestellten Speicherungsdauer automatisch wieder überschrieben.

Wird demgegenüber der Aufnahmemodus gestartet, so werden die zu diesem Zeitpunkt noch im RAM-Speicher der Kamera vorhandenen Aufnahmen dauerhaft abgespeichert und der Gesamtaufnahme vorangestellt. Auf diese Weise soll es der Polizei ermöglicht werden, auch solche Geschehnisse zu dokumentieren, die im Einzelfall erst zu der Situation geführt haben, in der der kameraführende Beamte den Einsatz der Bodycam zu einer dauerhaften Aufnahme für angebracht gehalten hat. Die Entwicklung des Einsatzgeschehens und die dokumentierten Straftaten sollen besser nachvollzogen werden können. Gleichzeitig soll die Gefahr von Fehlaufzeichnungen verringert werden, da der die Kamera tragende Beamte mehr Zeit für die Einschätzung hat, ob sich eine zunächst als gefährlich bewertete Lage tatsächlich in erwarteter Weise entwickelt.

Tatsächlich wird beim Prerecording also über einen nicht unerheblichen Zeitraum hinweg ein Lebenssachverhalt, bei dem nach Einschätzung des Polizeibeamten mit hinreichender Wahrscheinlichkeit eine Gefahr zu erwarten ist, in Ton und Bild mit einer Fülle personenbezogener Daten - auch unbeteiligter Dritter - aufgezeichnet und ggf. anschließend genutzt. Dieses Vorgehen haben wir im Gesetzgebungsverfahren kritisch herausgearbeitet. Mit Blick auf den Charakter dieser Regelung als der eines Pilotprojektes, das anders als in anderen Bundesländern direkt auf eine rechtliche Grundlage gestellt wird, haben wir uns aber entschieden, diese Regelung mitzutragen. Dies gilt insbesondere auch vor dem Hintergrund der in absehbarer Zeit vorzunehmenden Evaluierung des Projektes, bei der die Erforderlichkeit des „Pre-Recording“ besonders in den Blick genommen werden soll. Die Evaluation werden wir belgeiten.

6.2.2 Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz (BKAG)

Mit seinem Urteil vom 20. April 2016 zum BKAG führte das Bundesverfassungsgericht (BVerfG) seine ständige Rechtsprechung zu den Voraussetzungen für die Durchführung von hverdeckten Überwachungsmaßnahmen und zur weiteren Nutzung und Übermittlung der Daten zu anderen Zwecken an dritte Behörden systematisch zusammen und setzte neue Maßstäbe.

Das Urteil des BVerfG zum BKAG hat auch Auswirkungen auf das Sicherheits- und Ordnungsgesetz in Mecklenburg-Vorpommern (SOG M-V), welches die Ermittlungsbefugnisse der Polizei in Mecklenburg-Vorpommern regelt. Da das Bundesverfassungsgericht Vorgaben für die verfassungsmäßige Ausgestaltung von polizeilichen Eingriffsbefugnissen für Überwachungsmaßnahmen zum Zweck der Gefahrenabwehr oder Strafverfolgung und Datenübermittlungen sowie zweckändernde Datennutzungen gemacht hat und die Maßstäbe für die Zulässigkeit der Ausgestaltung der Ermittlungsbefugnisse bei verdeckt durchgeführter Überwachungsmaßnahmen zum Zweck der Gefahrenabwehr oder Strafverfolgung konkretisiert hat, stellt sich die Frage, ob das SOG M-V diesen Vorgaben aus dem Urteil stand hält. Das SOG M-V muss im Lichte der Entscheidung des BVerfG überprüft werden.

Gegenstand der Verfassungsbeschwerde waren vor allem zahlreiche Ermittlungsbefugnisse des Bundeskriminalamts nach dem BKAG - insbesondere Überwachungsmaßnahmen, Rasterfahndung, verdeckte Eingriffe in informationstechnische Systeme, die Überwachung der laufenden Telekommunikation sowie die Erhebung von Telekommunikationsverkehrsdaten. Das BVerfG erklärte einige Regelungen des BKAG für verfassungswidrig. Der Bundesgesetzgeber hat bereits vor dem Hintergrund dieses Urteils das BKAG novelliert, seit März 2017 ist ein grundsätzlich überarbeitetes BKA-Gesetz in Kraft.

Aus unserer Sicht sind die sich aus dem Urteil ergebenden Vorgaben des Bundesverfassungsgerichts für die verfassungsgemäße Ausgestaltung von polizeilichen Eingriffsbefugnissen und Datenübermittlungen sowie für zweckändernde Datennutzungen besonders bedeutsam für das SOG M-V. Sie sind im Folgenden zusammengefasst.

Das BVerfG hat befunden, dass nach Durchführung einer Wohnraumüberwachung eine unabhängige Stelle - außer bei Gefahr im Verzug - höchstpersönliche Informationen aus den Datensätzen herausfiltern muss, bevor sie verarbeitet werden dürfen, dieses müsse sichergestellt sein. Auch beim Zugriff auf informationstechnische Systeme muss ein hinreichender Schutz des Kernbereichs privater Lebensgestaltung sichergestellt sein, indem die die Daten unabhängig geprüft werden. Eine Sichtung durch Mitarbeiter der datenerhebenden Stelle genüge den Anforderungen nicht.

Sofern verdeckt durchgeführte Ermittlungsbefugnisse besonders tief in die Privatsphäre der Betroffenen eingreifen, ist es nach Auffassung des dem BVerfG Aufgabe des Gesetzgebers, einen angemessenen Ausgleich zwischen der Schwere des Grundrechtseingriffs einerseits und der Pflicht des Staates zum Schutz der Bevölkerung (Gefahrenabwehr und Strafverfolgung) andererseits zu schaffen. Der Verfassungsgrundsatz der Verhältnismäßigkeit verlange, dass derartigen Ermittlungsbefugnisse auf den Schutz gewichtiger Rechtsgüter begrenzt blieben. Im Gefahrenabwehrrecht seien sie nur dann verfassungsgemäß, wenn im Einzelfall eine Gefährdung der geschützten Rechtsgüter hinreichend konkret absehbar sei. Neben Zielpersonen dürfte sich die Maßnahme nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte erstrecken.

Weiter verweist das BVerfG darauf, dass der Einsatz von besonderen Mitteln zur Überwachung außerhalb von Wohnungen grundsätzlich einen Richtervorbehalt erfordere, sofern eine Datenerhebung durch langfristige Observation stattfinde oder nicht öffentliche Gespräche erfasst würden. Eine Wohnraumüberwachung bei Kontaktpersonen und Begleitpersonen sei unangemessen, weil eine derartige Maßnahme besonders tief in die Privatsphäre eindringe.

Nach dem Grundsatz der Zweckbindung dürfen Daten über das ursprüngliche Ermittlungsverfahren hinaus im Rahmen der festgelegten Zweckbestimmung weiter genutzt werden, solange die erhebungsberechtigte Behörde die Daten in demselben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutze. Damit verbunden sei eine Nutzung der Daten als bloßer Spurenansatz. Eine zweckändernde Nutzung der Daten habe sich dabei an dem sogenannten Grundsatz der hypothetischen Datenneuerhebung zu orientieren. Die neue Datennutzung müsse dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, das ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könne.

Das Kriterium der Datenneuerhebung gelte allerdings nicht schematisch abschließend und schließe die Berücksichtigung weiterer Gesichtspunkte nicht aus. Als neu zu rechtfertigender Eingriff bedürfe es eines eigenen, hinreichend spezifischen Anlasses. Dabei reiche aus, das sich aus den Daten - sei es aus ihnen selbst, sei es in Verbindung mit weiteren Erkenntnissen der Behörde - ein konkreter Ermittlungsansatz ergebe.

Bei Daten, die aus einer Wohnraumüberwachung oder einem Zugriff auf informationstechnische Systeme stammen, gelte für eine weitere oder zweckändernde Nutzung ein strengerer Maßstab. Hier müssten zusätzlich die für die Datenerhebung maßgeglichen Anforderungen an die Gefahrenlage erfüllt sein. Dies sei nur der Fall, wenn eine dringende oder im Einzelfall hinreichend konkretisierte Gefahrenlage vorliege.

Es bleibt abzuwarten, wie der Novellierungsbedarf für das Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern vor dem Hintergrund dieser Entscheidung des Bundesverfassungsgerichts ausgestaltet werden wird.

6.3 Justiz

6.3.1 Datenschutz in den Justizvollzugsanstalten in Mecklenburg-Vorpommern

Eine Petentin, die Mutter eines inhaftierten Gefangenen ist, berichtete uns, ihr Sohn habe in einer JVA des Landes eine Haftstrafe im offenen Vollzug verbüßt. Bei seiner Verlegung in eine andere JVA seien seine persönlichen Gegenstände von der Anstalt in Kartons verpackt und an sie übergeben worden. Dabei sei ihr aufgefallen, dass diese Kartons offensichtlich schon mehrfach für Haftumzüge anderer Häftlinge verwendet worden seien, ohne dass die alten Versandaufkleber entfernt wurden. Auf den Kartons hätten sich neben dem Versandaufkleber mit den Daten ihres Sohnes Versandaufkleber mit Daten von fünf weiteren Personen befunden. Es seien Namen, Vornamen, Geburtsdaten, Vorgangsnummern, die Angaben, von welcher JVA zu welcher JVA überführt wurde und die Hinweise „Strafhaft“ angegeben worden. Nach unserer Anfrage sagte die Justizvollzugsanstalt zu, in Zukunft grundsätzlich keine Kartons mit Adressaufklebern aus der JVA an Dritte oder Angehörige herauszugegeben. Für die Zukunft sei angewiesen worden, alle Hinweise auf persönliche Daten anderer Personen auf mehrfach benutzten Umzugskartons zu entfernen bzw. dauerhaft unleserlich zu machen. Wenn dies nicht möglich sein sollte, sind die Mitarbeiter angewiesen, die betreffenden Kartons im Rahmen der Aktenvernichtung zu entsorgen.

6.4 Kommunales

6.4.1 Ratsinformationssysteme auf Tablets

Regelmäßig werden wir von den Kommunen zum Thema Ratsinformationssysteme (RIS) konsultiert. Diese Systeme haben vielfältige Funktionen und dienen unter anderem als Informations- und Dokumentenmanagementsystem. Sie sollen den Mandatsträgern die aktuellen Drucksachen und Dokumente für die anstehenden Sitzungen in digitaler Form automatisiert bereitstellen und automatisiert Informationen für die Bürgerinnen und Bürger über das Internet zur Verfügung stellen. Ihr Einsatz steigert ohne Zweifel die Effizienz der Aufgabenerledigung der kommunalen Verwaltungen in der Vor- und Nachbereitung der Sitzungen.

Die Verfahren unterstützen darüber hinaus die ehrenamtliche Tätigkeit der Mandatsträger durch umfangreiche Recherche- und Archivfunktionen und erleichtern damit die Verwaltung der von den kommunalen Vertretungskörperschaften erstellten Drucksachen und Dokumente. Den ehrenamtlichen Mandatsträgern wird damit ein Arbeitsmittel an die Hand gegeben, mit dem sie effektiv auf die für ihre Tätigkeit notwendigen Dokumente zugreifen oder diese selbst erstellen und bearbeiten können. In vielen Fällen ist der Zugang zu den Systemen auch über das Internet vorgesehen, sodass die Mandatsträger sie bequem von zu Hause aus nutzen können. Diese Systeme werden inzwischen nicht nur mit dem klassischen PC oder dem Laptop bedient, sondern in zunehmendem Maße auch mit dem dienstlichen oder gar privaten Tablet.

Bei der Nutzung dieser modernen Informations- und Kommunikationstechniken muss aber beachtet werden, dass sie vielfältige Möglichkeiten bieten, personenbezogene Daten zielgerichtet auszuwerten und zu verarbeiten. Auch Ratsinformationssysteme können das Recht auf informationelle Selbstbestimmung der Betroffenen beeinträchtigen, etwa durch unzulässige Veröffentlichungen im Internet, durch unzureichende Zugriffskonzepte oder durch mangelnde Datensicherheit.

Unsere Erfahrungen zeigen, dass bei der Nutzung dieser Systeme in den Kommunen vielfach Unsicherheiten bestehen. Unklar ist oft, wem Zugriff auf die in den Systemen gespeicherten personenbezogenen Daten gewährt werden darf, welche personenbezogenen Daten in den RIS veröffentlicht werden dürfen und welche technischen und organisatorischen Maßnahmen zum Schutz der in den RIS verarbeiteten Daten zu treffen sind.

So müssen insbesondere die Vertraulichkeit und Integrität der in den RIS verarbeiteten personenbezogenen Daten gewährleistet werden, insbesondere bei nichtöffentlichen Dokumenten.

Vorgänge, die aufgrund berechtigter Interessen der Betroffenen in nichtöffentlicher Sitzung zu behandeln sind, dürfen ohne die vorherige Einwilligung der Betroffenen einer breiten Öffentlichkeit nicht zugänglich gemacht werden. Ihre Veröffentlichung im öffentlich zugänglichen Teil eines RIS ist daher nicht zulässig und muss mit geeigneten technischen und organisatorischen Maßnahmen verhindert werden. Derartige Vorgänge unterliegen auch der für ehrenamtliche Mandatsträger geltenden Amtsverschwiegenheit. Mandatsträger müssen deshalb auf ihre Rechte und Pflichten beim Umgang mit den RIS in besonderer Weise hingewiesen werden.

Grundsätzlich dürfen in RIS personenbezogene Daten nur verarbeitet werden, sofern dies für eine angemessene Information der Mandatsträger über den zur Beratung anstehenden Sachverhalt oder zur Unterrichtung der Einwohnerinnen und Einwohner erforderlich ist. Dies ergibt sich insbesondere aus den Grundsätzen der Erforderlichkeit und der Datenminimierung gemäß Artikel 5 Abs. 1 der Europäischen Datenschutz-Grundverordnung (DS-GVO).

Die Zugriffs- und Einsichtsrechte sind auf die jeweils übertragenen Aufgaben einzugrenzen (Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 DS-GVO). Für den Zugriff der Beschäftigten auf das Verfahren und deren Einsichtsrechte ist daher ein nach Schreib- und Leserechten differenziertes Berechtigungskonzept bzw. Rollenprofil zu erstellen.

Um geeignete und angemessene technische und organisatorische Maßnahmen auswählen zu können, ist vor der Einführung, Anwendung oder einer nachhaltigen Veränderung eines RIS eine Risikoanalyse vorzunehmen. Gegebenenfalls muss künftig auch eine Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO durchgeführt werden.

Auf der Grundlage der Risikoanalyse ist ein detailliertes Datenschutz- und Informationssicherheitskonzept zu erstellen um nachzuweisen, dass eine datenschutzkonforme und sichere Verarbeitung der personenbezogenen Daten stattfindet. Das betrifft sowohl Fragen der Sicherheit der Verarbeitung gemäß Art. 25 und 32 DS-GVO zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme als auch Fragen der Sicherstellung der Betroffenenrechte gemäß Art. 12, 13, 14 DS-GVO zur Wahrung der Transparenz, Zweckbindung und Intervenierbarkeit.

Besonders sorgfältig sind diese Maßnahmen beim Einsatz von mobilen Geräten wie Tablets auszuwählen, insbesondere dann, wenn damit nicht-öffentliche Dokumente verarbeitet werden sollen und diese Geräte dann auch noch privater Natur sind. Hierzu haben wir uns bereits im Zehnten (siehe Punkt 4.1.4) und Elften Tätigkeitsbericht (siehe Punkt 5.1.8) ausführlich geäußert. Wir empfehlen nachdrücklich den Einsatz von behördeneigenen Geräten. Nur so lassen sich rechtliche Vorgaben mit angemessenem Administrationsaufwand umsetzen. Die Administratoren müssen sich beispielsweise nicht mit den Betriebssystemen und Anwendungen, sogenannte Apps, unterschiedlicher Hersteller und den damit verbundenen, teils sehr unterschiedlichen Sicherheitsniveaus auseinandersetzen. Stattdessen kann gezielt das für den angestrebten Einsatzzweck geeignetste Endgerät und Betriebssystem sowie das dazu passende Mobile Device Managementsystem (MDM) ausgewählt werden, um so eine einheitliche und weitgehend administrierbare Systemumgebung für die mobilen Endgeräte zu schaffen.

Bei der Einführung eines RIS sollten unter anderem folgende Punkte mit behandelt und umgesetzt werden:

Information, Dokumentation und Schulung

- Das RIS ist umfassend zu dokumentieren; die genutzten Funktionalitäten sind transparent und verständlich darzustellen und in ihrer Bedienung allgemeinverständlich zu beschreiben. Die Nutzerinnen und Nutzer des Systems sind in die Bedienung einzuweisen; dabei ist auf mögliche Gefahren und Risiken sowie auf praktikable Möglichkeiten ihrer Reduzierung einzugehen.
- Art und Umfang der Nutzung des RIS sind verbindlich und für die Beschäftigten der Verwaltung nachvollziehbar in einer Dienstanweisung oder Dienstvereinbarung zu regeln.
- Die Verwaltung als Betreiberin des RIS ist verpflichtet, die Mandatsträger über die einzuhaltenden technischen und organisatorischen Maßnahmen zu informieren sowie alle Voraussetzungen zu schaffen, die den Mandatsträgern einen sicheren Umgang mit dem RIS ermöglichen.

Authentisierung und Rechteverwaltung

- Für die Gesamtanwendung ist eine hinreichende Nutzerauthentisierung sowie ein durchgreifendes Rechtekonzept zu entwickeln und technisch umzusetzen. Dabei ist sicherzustellen, dass nur Nutzerinnen und Nutzer Zugang zu dem System erhalten, die sich in geeigneter Weise beim System angemeldet haben und deren Berechtigung zweifelsfrei festgestellt worden ist.
- Durch geeignete Vergabe von Zugriffsrechten ist sicherzustellen, dass Nutzerinnen und Nutzer nur die Inhalte einsehen können, für die sie zugelassen worden sind, und nur Veränderungen an den Dokumenten vornehmen können, die ihren Aufgaben- oder Zuständigkeitsbereich umfassen. Die Umsetzung dieses Rechtekonzepts ist durch geeignete Maßnahmen sicherzustellen und stichprobenartig zu überwachen.
- Die Nutzung des Systems soll stets mit Standardrechten erfolgen; administrative Aufgaben bleiben speziellen Kennungen vorbehalten. Die Administration des Systems darf nur durch qualifiziertes Personal erfolgen; administrative Zugriffe, insbesondere soweit sie Änderungen an bestehenden Rechtekonzepten umfassen, müssen nachvollziehbar protokolliert werden.

Absicherung der Datenübertragung

- Soweit Nutzerinnen und Nutzern der Zugriff auf das System von Stellen außerhalb des lokalen Netzwerkes gewährt werden soll, sind eine gesicherte Übertragung der Daten über die externen Verbindungen sowie ein kontrollierter Zugang in das lokale Netzwerk zu gewährleisten. Als technische Mittel kommen hierfür insbesondere eine Verschlüsselung der Datenübertragung und die Absicherung des lokalen Netzes durch den Einsatz von geeigneter Firewall-Technologie in Betracht.
- Entsprechende Maßnahmen sind bei der Nutzung von E-Mail-Diensten zu ergreifen; auch hier kommt im Wesentlichen eine Verschlüsselung des Mail-Verkehrs in Betracht.
- Wird die Authentifikation der Nutzerinnen und Nutzer mit Hilfe von Chipkarten-Systemen vorgenommen, sollte die Nutzung dieser Systeme für den Einsatz der digitalen Signatur sowie der Verschlüsselung vorgesehen werden.

Nutzung von privaten Tablets, PC oder Laptops

- Sofern Mandatsträger mit eigenen privaten Geräten wie Tablets, PC oder Laptops von außerhalb auf das System zugreifen und Informationen aus dem System lokal speichern, sollte den Mandatsträgern angeboten werden, ihre Geräte vor der Nutzung von den Systemadministratoren der Verwaltung auf Sicherheitsmängel überprüfen zu lassen. Auf den Geräten ist ein Virenscanner einzusetzen, der regelmäßig aktualisiert wird. Die Aktualisierung der Virensignaturen und des verwendeten Betriebssystems ist möglichst automatisiert vorzunehmen.
- Werden sensitive Daten aus nichtöffentlichen Sitzungen auf Geräten außerhalb der Verwaltung gespeichert, sind diese Daten zwingend durch Verschlüsselungsverfahren nach dem Stand der Technik in geeigneter Weise gegen einen unbefugten Zugriff abzusichern.
- Dazu ist es erforderlich, auf den privaten Geräten Betriebssysteme zu verwenden, die eine Nutzerauthentifizierung ermöglichen und in der Lage sind, Rechtekonzepte wirkungsvoll umzusetzen.

- Darüber hinaus ist eine Verschlüsselung der aus dem RIS übertragenen Daten anzustreben.
- Sofern Mandatsträger ihre ehrenamtliche Tätigkeit beenden, ist sicherzustellen, dass die auf den heimischen oder mobilen Geräten gespeicherten vertraulichen Sitzungsunterlagen durch die Mandatsträger umgehend dauerhaft und unwiederbringlich gelöscht werden.
- Wegen der damit verbundenen besonderen Risiken für die Betroffenen sollte die Verarbeitung von personenbezogenen Daten gemäß Art. 9 DS-GVO, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie von Daten über Gesundheit oder Sexualleben, in RIS unterbleiben.

6.4.2 Datenerhebung durch kommunale Recyclinghöfe

Uns lagen mehrere schriftliche und telefonische Beschwerden zu einer Betreiberin von mehreren Recyclinghöfen vor, die seit Anfang des Jahres Daten von Abfallentsorgern erhebt. Hieraufhin baten wir die Betreiberin der Recyclinghöfe gemäß § 38 Abs. 3 Bundesdatenschutzgesetz (*BDSG*) um Stellungnahme und um Auskunft zum beschriebenen Sachverhalt.

Hiernach stellt sich der Sachverhalt wie folgt dar:

Die Betreiberin der Recyclinghöfe erklärte, dass die Recyclinghöfe nicht eigenwirtschaftlich, sondern im Auftrag der Hansestadt Rostock betrieben werden. Die Kosten für die Betreibung werden aus den von der Stadt erhobenen Abfallgebühren finanziert. Damit können gemeldete Einwohner der Hansestadt einige Abfallarten, weil durch die Abfallgebühren schon bezahlt, „kostenlos“ auf den Recyclinghöfen abgeben. Um Unberechtigte von der Nutzung dieser bereits bezahlten Leistung auszuschließen, hat die Hansestadt im Interesse der Gebührenpflichtigen die Betreiberin der Recyclinghöfe beauftragt, ein Annahmebuch einzuführen und die folgenden Daten zu erheben: Name des Recyclinghofs, Datum, Zeitpunkt, Wochentag der Anlieferung, Herkunft des Abfalls, Vorname, Nachname des Anlieferers, Kundennummer, Firmenname bei gewerblichen Anlieferern, Kfz-Kennzeichen bei Anlieferung mit Kfz, Vollmacht bei Anlieferung durch Dritte und Abfallart nach Abfallsatzung.

Zum Hintergrund des neu eingeführten Annahmebuches wurde erklärt, dass in den angrenzenden Landkreisen beispielsweise eine Grünschnittanlieferung vor Ort bezahlt werden muss, weil diese nicht in den Abfallgebühren der Landkreise enthalten ist. Dies hat in der Vergangenheit dazu geführt, dass zum Teil Bewohner aus den Landkreisen, aber auch Gewerbetreibende und andere Dritte (wie z. B. Hausmeisterdienste, Verwandte etc.) versucht haben, Abfall auf den Recyclinghöfen der Hansestadt kostenlos zu entsorgen. Bei den Recyclinghöfen der Hansestadt fällt eine gehäufte Anlieferung für einzelne Grundstücke nicht ohne Weiteres auf. Daher hat die Hansestadt entschieden, im Rahmen der elektronischen Erfassung eine Plausibilitätsprüfung für einzelne Grundstücke durchzuführen.

Die Rechtsgrundlage für die Erhebung und Verarbeitung der Daten der Hansestadtbewohner ergab sich aus der Abfallsatzung der Hansestadt i. V. m. der Abfallgebührensatzung der Stadt und dem Auftragsdatenverarbeitungsvertrag zwischen der Hansestadt als Auftraggeberin und der Betreiberin der Recyclinghöfe als Auftragnehmerin. Die Rechtsgrundlage für die Erhebung und Verarbeitung der Daten der anderen Betroffenen ergab sich aus § 28 Abs. 1 Nr. 1 *BDSG*.

6.4.3 Veröffentlichungen von Unterschriftenlisten bei Einwohneranträgen und Bürgerbegehren im Internet

Die Kommunalverfassung Mecklenburg-Vorpommern sieht eine Reihe von Möglichkeiten der Einwohnerbeteiligung vor. Hierunter fallen unter anderem sogenannte Einwohneranträge und Bürgerbegehren. Mit einem Einwohnerantrag soll erreicht werden, dass durch eine Gemeindevertretung eine wichtige Angelegenheit des eigenen Wirkungskreises behandelt wird. Durch ein Bürgerbegehren hingegen soll die Durchführung eines Bürgerentscheides erreicht werden.

Bei beiden Beteiligungsmöglichkeiten sind bestimmte formale Anforderungen einzuhalten. Insbesondere bedarf es hierzu einer Unterschriftenliste, in der neben der jeweiligen Unterschrift auch Familienname, Vorname, Geburtsdatum, Anschrift sowie Datum der Unterzeichnung lesbar einzutragen sind. Über die Zulässigkeit eines Einwohnerantrages oder Bürgerbegehrens entscheidet dann die Gemeindevertretung.

Im Berichtszeitraum wurden wir darüber in Kenntnis gesetzt, dass sowohl bei einem Einwohnerantrag als auch bei einem Bürgerbegehren die vollständigen Unterschriftenlisten im Internet veröffentlicht wurden. Mit dieser Veröffentlichung im Internet wollte man unter Nutzung moderner und zeitgemäßer Kommunikationsmittel dem Öffentlichkeitsgebot Rechnung tragen und somit auch den Grundsatz der Transparenz weiter stärken. Von daher war das Ansinnen der Verwaltungstransparenz durchaus positiv zu werten. Dieses schließt jedoch nicht automatisch die Veröffentlichung der vorgenannten personenbezogenen Daten ein. Vielmehr bedarf es hierzu einer entsprechenden Rechtsvorschrift beziehungsweise einer ausdrücklichen Einwilligungserklärung. Beides lag jedoch nicht vor.

In einem der beiden Fälle wurde uns vielmehr entgegengehalten, dass die Personen durch ihre Unterschriftsleistung aus eigenem Antrieb heraus freiwillig die Öffentlichkeit suchen würden und somit schlussfolgernd die Einwilligung vorliegen würde. Diesem haben wir widersprochen, da sich die Unterschrift auf dem Einwohnerantrag beziehungsweise dem Bürgerbegehren auf den zugrundeliegenden Zweck bezieht und eine Verarbeitung zu anderen Zwecken nicht beinhaltet.

Die vorgenommenen Veröffentlichungen der Unterschriftenlisten im Internet waren aus unserer Sicht rechtswidrig. Neben der Rechtswidrigkeit könnten diese Veröffentlichungen eine durchaus abschreckende Wirkung auf Personen, die sich derartiger Möglichkeiten der Beteiligung an kommunalen Entscheidungen bedienen wollen, haben. Nicht jeder, der eine Unterschrift leistet und dabei auch noch bestimmte seine Person betreffende Daten angeben muss, möchte, dass diese Informationen zweckentfremdet einer breiten Öffentlichkeit zur Verfügung gestellt werden.

Wir haben deshalb in beiden Fällen die Empfehlung gegeben, die Unterschriftenlisten unverzüglich und unwiederbringlich aus den Internetpräsentationen zu löschen. Eine der beiden Verwaltungen ist diesem unmittelbar gefolgt. In dem anderen Fall konnte bislang noch kein abschließendes Ergebnis herbeigeführt werden.

6.4.4 Umgang mit Traueranzeigen

Eine Petentin informierte uns darüber, dass im Lokalteil einer Tageszeitung seit geraumer Zeit unter der Rubrik „Unser Beileid“ Traueranzeigen veröffentlicht werden, in denen unter anderem auf Beisetzungen und Trauerfeiern hingewiesen wird. Die Hinterbliebenen wurden dabei nicht gefragt, ob sie dies wollen oder nicht. Stattdessen stammen diese Informationen von Aushängen, die auf dem Friedhof vorgenommen wurden. In diesen Mitteilungen sind neben den Vor- und Nachnamen der Verstorbenen auch Angaben zum Zeitpunkt und Ort der Trauerfeier enthalten.

Nach Auskunft der zuständigen Friedhofsverwaltung werden die Hinweise auf Trauerfeiern jeden Morgen neu ausgehängt und nach der letzten Trauerfeier abgenommen. Die Notwendigkeit des Aushangs wird damit begründet, dass diese Vorgehensweise für die Aufrechterhaltung der Abläufe auf dem Friedhof und speziell für die Feierhallen unerlässlich sei. Sie dient der Nutzerführung, damit die Trauernden informiert werden, wann die Trauerfeier beginnt und wo sie sich einzufinden haben (in einer der Feierhallen, vor der Feierhalle oder direkt an der Grabstelle), um von den Verstorbenen Abschied nehmen zu können. Außerdem sei der Aushang für Trauergäste, die im Vorfeld keine konkreten Informationen erhalten haben oder sich nicht sicher sind, häufig die einzige Informationsquelle.

Nach der für den Friedhof geltenden Friedhofssatzung dürfen personenbezogene Daten beispielsweise zur Bewirtschaftung und Verwaltung der Friedhöfe verarbeitet werden. Auch wenn die von der Friedhofsverwaltung vorgetragene Erforderlichkeit der Aushänge plausibel scheint, bedarf es hierzu einer legitimierenden Rechtsvorschrift oder der Einwilligung. Dieses ist allein schon dem Umstand geschuldet, dass nicht alle Hinterbliebenen einen derartigen öffentlichen Hinweis auf ihre Trauerfeier und sich daraus ergebender Veröffentlichung in einer Zeitung wollen.

Da die in der Friedhofssatzung getroffenen Regelungen zur Datenverarbeitung nicht ausreichen, haben wir der Friedhofsverwaltung empfohlen, künftig von den Hinterbliebenen die Einwilligung zum öffentlichen Aushang einzuholen. Dieser Empfehlung wurde gefolgt.

6.5 Soziales/Arbeitnehmerdatenschutz

6.5.1 Landkreis verlangt vom Sozialhilfeträger eine Erklärung zur Offenlegung der Einkommens- und Vermögensverhältnisse

Ein Petent schilderte uns, dass er Sozialleistungen nach dem Sozialgesetzbuch XII (SGB XII) beantragt habe. In diesem Zusammenhang sei er vom Landkreis aufgefordert worden aufzulisten, bei welchen Geldinstituten er Bankverbindungen unterhalte. Es sei ihm auch eine Erklärung ausgehändigt worden, in der insbesondere die Bankverbindung, Kontonummer, Sparkonto, Girokonto, Wertpapier oder andere Sparformen angegeben werden sollte. Des Weiteren sei er aufgefordert worden, die genannten Geldinstitute zu ermächtigen, gegenüber dem jeweiligen Sozialhilfeträger uneingeschränkt Auskunft über die Konten, deren Bestände sowie gegebenenfalls den Umfang der Kontenbewegung des letzten halben Jahres zu erteilen. Der Petent bat uns, den Sachverhalt datenschutzrechtlich zu bewerten.

Wir haben uns zunächst an den Landkreis gewandt und gefragt, ob eine entsprechende Erklärung von allen Personen, die Leistungen nach dem SGB XII beantragt haben, verlangt wird bzw. falls nicht, nach welchen Kriterien entschieden wird, wer eine solche Erklärung auszufüllen hat und zu welchem Zweck die Entbindung der Geldinstitute von der Schweigepflicht regelmäßig erforderlich ist.

Vom Landkreis erhielten wir die Auskunft, dass die entsprechende Erklärung von allen Personen verlangt wird, die erstmals eine Leistung nach dem SGB XII beantragen, sofern diese einkommens- und vermögensabhängig ist. Diese Erklärung wird den Antragstellern zusammen mit dem Sozialhilfeantrag zugeschickt und ist Bestandteil der Unterlagen. Rechtlich hat der Landkreis diese Datenerhebung auf § 60 Sozialgesetzbuch Erstes Buch (SGB I) gestützt.

Auch wenn § 60 Abs. 1 Satz 1 SGB I grundsätzlich eine Mitwirkungspflicht des Antragstellers von Sozialleistungen auch in Bezug auf die Erteilung von erforderlichen Auskünften durch Dritte erfordert, sind dieser Mitwirkungspflicht Grenzen gesetzt. Wie die Pflicht zur Angabe bestimmter Tatsachen besteht auch die Pflicht zur Zustimmung von Auskünften nur dann, wenn dies für die konkrete Sozialleistung erforderlich ist.

Für den uns geschilderten Sachverhalt bedeutete dies, dass so weitreichende Daten nur zu erheben sind bzw. die entsprechende Einwilligung in die Auskunftserteilung lediglich dann verlangt werden darf, wenn dies in dem konkreten Einzelfall für die Erbringung der konkreten Sozialleistung unverzichtbar ist. Entsprechend dem datenschutzrechtlichen Grundsatz der Ersterhebung beim Betroffenen hätte der Sozialleistungsträger zunächst prüfen müssen, ob die Frage zu der Einkommens- und Vermögenssituation nicht durch die Vorlage anderer Unterlagen beantwortet werden kann. Dieser Grundsatz darf nicht von vornherein durch die Einholung einer Einwilligungserklärung umgangen werden. Erst wenn der Betroffene nicht hinreichend mitwirkt oder wenn berechtigte Zweifel an der Richtigkeit seiner Angaben vorliegen, ist es verhältnismäßig, zu Mitteln zu greifen, aufgrund derer der Antragsteller entscheiden muss, ob er geheimhaltungsbedürftige Tatsachen preisgeben möchte oder die Versagung der Leistung riskiert.

Aus datenschutzrechtlicher Sicht ist eine pauschale, undifferenzierte Forderung zur Abgabe solcher Erklärungen, auch bei erstmaliger Stellung eines Antrages, zu weitreichend.

Wir haben dem Landkreis daher empfohlen, die in Rede stehende Einwilligungserklärung nicht generell bei allen Erstantragstellern zu verwenden, sondern zunächst den Antragsteller selbst zu befragen und entsprechende Unterlagen, wie Kontoauszüge, zu verlangen. Selbst hier darf der Antragsteller in bestimmten Fällen gewisse Schwärzungen vornehmen und ist darauf hinzuweisen. Näheres hierzu ist auf unserer Internetseite unter dem Punkt „Datenschutz/Publikationen/Broschüren“ zu finden.

Der Landkreis teilte uns daraufhin mit, dass man unserer Argumentation folgt und im Ergebnis die in Rede stehende Erklärung ab sofort nicht mehr verwenden wird. Zudem wurde sie auf der Internetseite des Landkreises aus den dort bereitgestellten Antragsunterlagen entfernt.

6.6 Gesundheitswesen

6.6.1 Entwicklung des Krebsregisterrechts im Berichtszeitraum

Am 11. Juli 2016 ist das neue Gesetz über die Krebsregistrierung in Mecklenburg-Vorpommern (Krebsregistrierungsgesetz KrebsRG M-V), veröffentlicht im GVOBl. M-V S. 539, in Kraft getreten und gilt seit dem 31. Dezember 2016 (zur Vorgängerregelung siehe Elfter Tätigkeitsbericht, Punkt 6.6.2). Wir haben das Gesetzgebungsverfahren begleitet und in Anhörungen Stellung genommen. Anpassungen an die ab dem 25. Mai 2018 geltende Datenschutz-Grundverordnung sind noch im Berichtszeitraum vorbereitet worden und können voraussichtlich rechtzeitig bis Mai 2018 vom Landtag Mecklenburg-Vorpommern verabschiedet werden.

Das Gesetz unterscheidet zwischen einem klinischen und einem epidemiologischen Krebsregister. Die klinische Krebsregistrierung dient der Verbesserung der Qualität der onkologischen Versorgung. Ärzte, Ärztinnen, Zahnärzte, Zahnärztinnen, Krankenhäuser sowie andere ärztliche Einrichtungen, die an der Krankenversorgung teilnehmen, sind nach dem Gesetz verpflichtet, Befund und Therapie an das Krebsregister zu melden und die Patienten über die Krebsregistrierung aufzuklären. Der Patient kann einer Registrierung gegenüber der zur Meldung verpflichteten Stelle aber grundsätzlich widersprechen. In diesem Fall werden die Daten gelöscht, die nicht auch für das epidemiologische Krebsregister benötigt werden. Epidemiologische Krebsregister erfassen, wie häufig Krebs in Deutschland auftritt. Für Mecklenburg-Vorpommern übernimmt dies das Gemeinsame Krebsregister mit Sitz in Berlin. Die Meldung zum epidemiologischen Krebsregister ist verpflichtend; eine Widerspruchsmöglichkeit ist nicht vorgesehen.

Klinische Krebsregister gibt es auch in anderen Bundesländern. Ein Austausch zwischen den Registern ist in bestimmten Fällen möglich und auch vorgesehen. Es kann daher vorkommen, dass personenbezogene Daten über einen Patienten in mehreren Krebsregistern gespeichert sind, beispielsweise, weil sich der Patient in Mecklenburg-Vorpommern, Schleswig-Holstein und Hamburg behandeln lässt. Umso wichtiger es, dass auch die Datenschutz-Aufsichtsbehörden der Länder bei der Beratung ihrer jeweiligen Register zusammenarbeiten. Wir nehmen am Arbeitskreis Gesundheit und Soziales teil, der sich auch zum Thema Krebsregister austauscht. Ein wichtiges Thema ist hier beispielsweise, wie ein einmal erhobener Widerspruch gegenüber allen klinischen Krebsregistern durchgesetzt werden kann.

Darüber hinaus kontrollieren wir die beteiligten Stellen anlasslos und überprüfen, ob die nach dem Gesetz vorgesehenen Maßnahmen zum Schutz dieser sensiblen Gesundheitsdaten umgesetzt werden.

Wir sind zudem im Beirat vertreten und werden auch das weitere Gesetzgebungsverfahren begleiten. An den vorgesehenen Änderungen kritisieren wir insbesondere, dass nur zum Zweck der Abrechnung zwischen dem Krebsregister und den Krankenkassen bestimmte technische und organisatorische Maßnahmen außer Kraft gesetzt werden sollen, die bisher ganz wesentlich zu einem hohen Schutzniveau für die sensiblen Daten beigetragen haben.

6.6.2 Zusammenfassung verschiedener Beratungen im Telemedizinbereich

Wir haben im Berichtszeitraum verschiedene Initiativen zu Telemedizin und Gesundheitsnetzwerken beraten, noch bevor diese starteten. Gerade in einem Flächenland wie Mecklenburg-Vorpommern kann mehr Digitalisierung im Gesundheitswesen zu einer besseren Versorgung beitragen. Allerdings müssen hier Chancen und Risiken abgewogen werden. Wir haben bei diesen informellen Vorabprüfungen insbesondere technische und organisatorische Maßnahmen einer summarischen Prüfung unterzogen. Bei mehreren Projekten fiel auf, dass aber vor allem bei der Transparenz noch Nachbesserungsbedarf bestand. Teilnehmer an Gesundheitsnetzwerken oder telemedizinischen Angeboten müssen leicht nachvollziehen können, wer was wann und auf welcher Grundlage mit ihren personenbezogenen Daten macht und wie sie darauf Einfluss nehmen können. Auch die Frage, wer in einem Netzwerk wofür verantwortlich ist und den betroffenen Personen als Ansprechpartner zur Verfügung steht, wird kontrovers diskutiert. Skeptisch stehen wir Projekten gegenüber, bei denen die Datenverarbeitung so organisiert ist, dass die empfindlichen Gesundheitsdaten in Ländern außerhalb der Europäischen Union verarbeitet werden. Dies ist nicht per se verboten, bedarf aber einer gesonderten rechtlichen Prüfung und Risikoabwägung. Zudem muss verhindert werden, dass über Netzwerke Gesundheitsdaten zur Bemessung von Versicherungstarifen laufend erhoben und vertragsbegleitend genutzt werden können. Eine zentrale Forderung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder verlangt in den „Grundsatzpositionen und Forderungen für die neue Legislaturperiode“, dass bei der Bemessung von Versicherungstarifen nicht die Patienten und Versicherten benachteiligt werden, die einer umfassenden Erfassung und Übertragung von Gesundheitsdaten nicht zustimmen.

Wir sind auch zu diesem Thema in länderübergreifenden Arbeitskreisen aktiv. Hier werden grundsätzliche Positionen abgestimmt. Wir verfolgen dabei ein erklärtes Ziel: Datenschutz soll die Digitalisierung im Gesundheitswesen nicht verhindern, sondern besser machen!

6.6.3 Fragebogenaktion zum Stand der Anpassung der Praxisorganisation an die Datenschutz-Grundverordnung

Ab dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung in allen Mitgliedstaaten der Europäischen Union unmittelbar und überall. Auch Ärztinnen und Ärzte in Mecklenburg-Vorpommern treffen dann u. a. umfangreiche Dokumentationspflichten zum Datenschutz. Neu ist vor allem, dass Patienten bestimmte Informationen zur Datenverarbeitung, beispielsweise zur Dauer der Aufbewahrung von Patientenakten, mitzuteilen sind. Diese Informationen muss mit der Datenerhebung zur Verfügung gestellt werden - unabhängig davon, ob der Patient danach fragt. Das gilt auch, wenn die Datenverarbeitung nicht auf einer Einwilligung, sondern einer anderen Rechtsgrundlage beruht. Den Arztpraxen droht mit Geltung der Datenschutz-Grundverordnung auch ein hohes rechtliches Risiko, wenn Zuwiderhandlungen gegen diese Pflichten durch die Aufsichtsbehörde mit empfindlichen Bußgeldern sanktioniert werden müssen oder Patientinnen und Patienten im Zivilrechtsweg gegen Datenpannen vorgehen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern möchte den Ärztinnen und Ärzten im Land beratend zur Seite stehen, damit es zu Verstößen gar nicht erst kommt. Um hier Problemschwerpunkte identifizieren und gezielter Schulungen und Beratungen anbieten zu können, hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern im Dezember 2017 an mehr als 200 zufällig ausgewählte Ärztinnen und Ärzte Fragebögen versandt.

Diese enthielten bewusst teilweise schwierige Formulierungen aus der Datenschutz-Grundverordnung, um einen Einblick darüber zu gewinnen, ob das neue Gesetz schon bei allen Anwendern angekommen ist. Zudem war der Fragebogen so konzipiert, dass mit der Beantwortung nicht gegen die geltende Rechtslage verstoßen werden konnte. Die Auswertung der Fragebögen wurde so geplant, dass die Antworten zwar hinsichtlich des Schulungsbedarfs, nicht aber zur Kontrolle der Ärzte erfasst werden. Die Auswertung ist voraussichtlich im 1. Quartal des neuen Berichtszeitraums abgeschlossen.

6.6.4 Befundanforderungen durch das Landesamt für Gesundheit und Soziales

In Vorträgen und Schulungen gegenüber Berufsgeheimnisträgern weist der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern häufig auch auf das Berufsgeheimnis nach § 203 Strafgesetzbuch sowie die korrespondierenden Zeugnisverweigerungsrechte und Beschlagnahmeverbote in dem jeweiligen Verfahrensrecht hin. Dass personenbezogene Daten nicht einfach so an andere Stellen, seien es Behörden oder Unternehmen, übermittelt werden dürfen, wird allgemein in Datenschutzschulungen betont. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern begrüßt es daher, wenn Ärzte und Krankenhäuser kritisch hinterfragen, ob dem Landesamt für Gesundheit und Soziales Befunde von Patienten, etwa zur Feststellung einer Behinderung, übermittelt werden dürfen, ohne das die Behörde mit der Anforderung des Befundes eine Schweigepflichtsentbindungserklärung übersendet. In diesem speziellen Fall vertritt der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern jedoch die Auffassung, dass eine gesetzliche Befugnis zur Offenbarung besteht und insoweit kein Einverständnis des Antragstellers bei der Befundanforderung mitübersandt werden muss. In der Befundanforderung muss die Behörde jedoch mitteilen, nach welcher gesetzlichen Grundlage der Arzt oder Angehörige eines anderen Heilberufs zur Auskunft verpflichtet sein soll.

6.6.5 Umgang mit Patientenakten/Patientendokumentationen

Im Berichtszeitraum wandte sich ein Mitarbeiter einer Rehaklinik an uns, weil er nach einer Stationsversammlung zum Thema Patientendokumentation ein „ungutes Gefühl“ hinsichtlich der Aufbewahrung der Patientendokumentationen in den Krankenzimmern hatte. Er bat uns um eine datenschutzrechtliche Einschätzung.

Patientendaten unterliegen einem besonderen Schutz, dem Patientengeheimnis, welches seine Grundlage in verschiedenen Rechtsbereichen findet, Berufsordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern (BÄO M-V), Bürgerliches Gesetzbuch (BGB), Strafgesetzbuch (StGB) oder im Datenschutzrecht. So stellt § 203 StGB die unbefugte Offenbarung von Patientendaten unter Strafe, das heißt Geldstrafe oder sogar bis zu zwei Jahre Gefängnis. Nicht nur Ärztinnen und Ärzte müssen das Patientengeheimnis wahren, sondern auch Krankenschwestern und Krankenpfleger sowie Hebammen, Logopädinnen/Logopäden, Ergotherapeutinnen/Ergotherapeuten und andere sogenannte Berufsgeheimnisträger.

Von einer befugten Offenbarung, zum Beispiel der Übermittlung von Patientendaten an Dritte, kann man nur ausgehen, wenn eine Rechtsvorschrift dies ausdrücklich zulässt oder der betroffene Patient darin eingewilligt hat. Des Weiteren hat die datenverarbeitende Stelle, hier die Rehaklinik, dafür Sorge zu tragen, dass nur befugte Personen Zugang zu den Patientendokumentationen haben. Befugt ist nur die Person, die mit der Pflege des Patienten beauftragt ist. Dies wird in der Regel durch entsprechende technische und organisatorische Maßnahmen gewährleistet, zum Beispiel sollte die Patientendokumentation so aufbewahrt werden, dass nur die mit der Behandlung des Patienten befassten Personen auf diese zugreifen können.

Im Rahmen des vom Mitarbeiter der Rehaklinik erwähnten Planettensystems werden die anfallenden Befunde in einer Befundtasche (Planette) geordnet abgeheftet, sodass ein schneller und direkter Zugriff auf die Patientendaten möglich ist. Allerdings sind die Planetten nicht besonders gesichert, sodass jeder, der in das Krankenzimmer kommt, auf diese Daten zugreifen könnte und somit die Möglichkeit besteht, dass Daten von unberechtigten Personen zur Kenntnis genommen, geändert oder ausgetauscht werden.

Außerdem ist es den Patienten nicht immer möglich zu prüfen, ob jemand berechtigt ist, die Dokumentation einzusehen und Daten einzutragen, sodass auch die Integrität der Dokumentation gefährdet wird, weil Dokumente ohne Kontrolle ausgetauscht oder vernichtet werden könnten.

Aus diesen Gründen haben wir es einvernehmlich für nicht zulässig bewertet, die Pflegedokumentation am Patientenbett, auch nicht mit Hilfe des Planettensystems, aufzubewahren.

6.7 Finanzwesen

6.7.1 Kopieren von Personalausweisen beim Schrotthandel als Nachweis für das Finanzamt?

Im Rahmen einer Petition sind wir darauf aufmerksam geworden, dass es verbreitet zu sein scheint, beim Ankauf von Altmetallen zum Zwecke der steuerlichen Berücksichtigung der Ausgaben die Ausweise der Zahlungsempfänger zu kopieren. Die Kopien würden angefertigt werden, da man sich unsicher sei, welcher Nachweis zur Person des Zahlungsempfängers für eine steuerliche Berücksichtigung durch die Finanzbehörden nach § 160 Abgabenordnung (AO) erforderlich sei.

Gemäß § 60 AO sind Schulden und andere Lasten, Betriebsausgaben, Werbungskosten und andere Ausgaben steuerlich regelmäßig nicht zu berücksichtigen, wenn der Steuerpflichtige dem Verlangen der Finanzbehörde nicht nachkommt, die Gläubiger oder die Empfänger genau zu benennen.

Vor dem Hintergrund dieser Regelung, die nicht auf das Fertigen einer Ausweiskopie abstellt, haben wir das Finanzministerium dazu befragt, welche Nachweise die Finanzbehörden in Mecklenburg-Vorpommern zur Person des Zahlungsempfängers zum Zweck der steuerlichen Berücksichtigung der Ausgaben fordern.

Das Finanzministerium hat hierzu mitgeteilt, dass das Thema in jüngster Zeit bei den obersten Finanzbehörden des Bundes und der Länder intensiv erörtert worden sei. Im Ergebnis der unter Einbeziehung entsprechender Stellungnahmen des BMI geführten Erörterungen vertritt das Finanzministerium die Auffassung, dass es nicht zulässig sei, vom Steuerpflichtigen zum Zweck der Benennung und mithin des Nachweises von Gläubigern bzw. Zahlungsempfängern die Erstellung einer Kopie von deren Personalausweisen für steuerliche Zwecke zu verlangen. Inhaltliche Anforderung an die Benennung des Gläubigers bzw. Zahlungsempfängers sei laut § 160 AO lediglich eine „genaue“ Benennung. Das bedeute, dass ein Zahlungsempfänger im Einzelfall so genau bezeichnet werden muss, dass die Finanzbehörde ohne besondere Schwierigkeiten und ohne Zeitaufwand in der Lage ist, den Empfänger zu ermitteln. Ausreichend sei zum Beispiel die Vorlage des Personalausweises und Aufzeichnungen der nach § 160 AO zu erfassenden Daten.

Nach Kenntnis des Finanzministeriums hätten zwar in Einzelfällen Schrotthändler (mit Einverständnis der Anlieferer) Kopien von Personalausweisen zu ihren Unterlagen genommen. Grund hierfür sei auch, dass sich die Schrotthändler wegen der hohen Anzahl von Diebstählen in diesem Bereich selbst absichern wollten, um bei laufenden behördlichen Überprüfungen nicht als Hehler in Verdacht zu kommen.

Wir teilen die Auffassung des Finanzministeriums und haben den Petenten darüber in Kenntnis gesetzt. Das Finanzministerium hat zugesagt, die Finanzämter im Sinne dieser Auffassung zu unterrichten.

6.7.2 Support für Steuerverfahren ohne Rechtsgrundlage

2016 teilte uns das Finanzministerium mit, dass die Finanzverwaltung Mecklenburg-Vorpommerns für eine ihrer Fachanwendungen Support aus einem anderen Bundesland in Anspruch nehmen wolle. Das Verfahren für den Support, genannt länderübergreifende gebündelte Verfahrensbetreuung (LGVB), solle gleichzeitig als Pilotprojekt für andere Fachverfahren dienen.

Bei derartigen Supportleistungen ist es unvermeidlich, dass die Support leistende Stelle auf Steuerdaten zugreifen kann. Steuerdaten unterliegen dem besonderen Schutz des Steuergeheimnisses (§ 30 AO), das auch innerhalb der Finanzverwaltung gilt. Es fand sich aber keine passende Rechtsvorschrift, auf die eine Offenbarung von Steuerdaten an Stellen anderer Bundesländer zu Zwecken des technischen Supports hätte gestützt werden können. Insbesondere ist eine Offenbarung an Stellen anderer Bundesländer nicht aufgrund von § 30 Abs. 4 Nr. 1 AO („soweit [die Offenbarung] der Durchführung eines Verfahrens im Sinne des Absatzes 2 Nr. 1 Buchstaben a und b dient“) zulässig, denn diese Stellen sind im Rahmen der üblichen Bearbeitung von Stundungs- und Erlassfällen oder anderen Besteuerungsverfahren nicht zuständig.

Durch Abschluss eines Vertrags nach § 4 DSG M-V konnte dieser Mangel nicht geheilt werden. Ein Staatsvertrag, der als Rechtsgrundlage hätte dienen können, befand sich noch im Rechtsetzungsverfahren.

Dass es sich bei dem Vorhaben der Finanzverwaltung um einen Prototypen handeln sollte, ändert daran nichts. Verarbeitungen personenbezogener Daten sind in einem Test- oder Pilotbetrieb nicht risikoärmer für die betroffenen Personen als im Wirkbetrieb. Wir haben das Finanzministerium auf diesen Umstand hingewiesen.

Trotz fehlender Rechtsgrundlage nahm die Finanzverwaltung das beschriebene Support-Verfahren im April 2017 in Betrieb.

Hierzu haben wir das Finanzministerium zur Stellungnahme aufgefordert. Uns sind jedoch keine überzeigenden Gegenargumente vorgetragen worden. Daraufhin haben wir von einer Beanstandung lediglich vorläufig abgesehen, weil die Rechtswidrigkeit durch den geplanten Staatsvertrag in der uns vorliegenden Entwurfsfassung abgestellt würde.

Zum Ende des Berichtszeitraums war das Rechtsetzungsverfahren noch nicht abgeschlossen.

6.8 Bildung

6.8.1 Datenschutz in den Schulen

Projekt „Datenschutz an den Schulen in Mecklenburg-Vorpommern“

Das Projekt „Datenschutz an den Schulen in Mecklenburg-Vorpommern“ haben wir 2014/2015 durchgeführt und über erste Zwischenergebnisse bereits im Zwölften Tätigkeitsbericht informiert, siehe dort Punkt 2.1.5.

Ziel des Projektes war es, den Stand der Umsetzung des Datenschutzes an den Schulen in Mecklenburg-Vorpommern zu ermitteln. Im Frühjahr 2016 haben wir die Ergebnisse der Erhebung in einem umfassenden Projektbericht veröffentlicht[21].

Nach Auswertung der Ergebnisse war festzustellen, dass die Datenschutzvorschriften an der überwiegenden Zahl der Schulen des Landes nicht ausreichend umgesetzt werden. Um das Datenschutzniveau an den Schulen zu verbessern, haben wir unter anderem folgende Empfehlungen ausgesprochen:

- das Schulgesetz Mecklenburg-Vorpommern ist aus datenschutzrechtlicher Sicht zu novellieren,
- die Schulen sind mit finanziellen Mitteln für den technischen Datenschutz auszustatten,
- die für den Datenschutz Verantwortlichen in den Schulen sind zu schulen,
- die für die Schulen erforderlichen behördlichen Datenschutzbeauftragten sind beim Schulträger, deren Stellvertreter bei der jeweiligen Schule zu bestellen,
- die dienstliche Nutzung von privaten Datenverarbeitungsanlagen der Lehrkräfte ist mit dem Ziel einer datenschutzgerechten Datenverarbeitung neu zu regeln,
- schon bei der Planung einer landeseinheitlichen Schulverwaltungssoftware sind datenschutzrechtliche Mindeststandards zu berücksichtigen,
- die elektronische Aufbewahrung und Archivierung von schulischen Akten ist zu regeln.

[21] https://www.datenschutz-mv.de/static/DS/Dateien/Themen/pb-ds-schulen.pdf.

Den Projektbericht haben wir auf einer Landespressekonferenz gemeinsam mit dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, dem Landkreistag Mecklenburg-Vorpommern e. V. und dem Städte- und Gemeindetag Mecklenburg-Vorpommern e. V. am 26. April 2016 in Schwerin der Öffentlichkeit vorgestellt. Unsere oben genannten Empfehlungen hatten wir schon vor der Pressekonferenz mit allen Beteiligten besprochen. In den Gesprächen wurde klar, dass die datenschutzrechtlichen Defizite nur durch gemeinsames Handeln beseitigt werden können. Das betrifft sowohl die rechtlichen Aspekte der Novellierung als auch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen. Daher wurde vereinbart, dass die identifizierten datenschutzrechtlichen Probleme zunächst an dafür ausgewählten Musterschulen gelöst werden sollen. Um ressourcenschonend zu arbeiten, sollen dies dieselben Musterschulen wie aus dem Projekt Arbeitsgruppe „Digitale Schule“ sein.

Arbeitsgruppe „Digitale Schule„

Um die Kooperationsvereinbarung zur Medienkompetenzförderung vom April 2015 umzusetzen, wurde unter anderem die Arbeitsgruppe „Digitale Schule“ gegründet. Sie hatte das Ziel, der Landesregierung und den kommunalen Schulträgern bis Anfang 2017 einen Orientierungsrahmen für eine nachhaltige Strategie in Bezug auf eine angemessene Ausstattung der Schulen mit Informationstechnik (IT) zu bieten. Bereits im Zwölften Tätigkeitsbericht haben wir darüber berichtet, siehe dort Punkt 2.1.2.

Bis Redaktionsschluss dieses Tätigkeitsberichtes konnte die Arbeitsgruppe jedoch weder der Landesregierung noch den kommunalen Schulträgern Arbeitsergebnisse vorlegen, die als Orientierungsrahmen für eine nachhaltige Strategie in Bezug auf eine angemessene Ausstattung der Schulen mit Informationstechnik dienen. Ein Grund für die Verzögerung war, dass sich die Bewilligung für den finanziellen Rahmen des Projektes als sehr zeit- und verhandlungsintensiv darstellte. Andere Gründe für den Zeitverzug lagen in der Suche nach einem geeigneten Projektträger aus der Mitte der Schulträger sowie der Organisationsumgestaltung im Ministerium für Inneres und Europa Mecklenburg-Vorpommern sowie dem Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern nach den Landtagswahlen. Erst Ende 2017 wurde ein geeigneter Projektträger gefunden.

Bis zum Ende dieses Berichtszeitraumes hatten sich fünf Schulen bereiterklärt, im Rahmen des Projektes der AG „Digitale Schule“ mitzuwirken. An diesen Schulen soll der Orientierungsrahmen für eine nachhaltige Strategie in Bezug auf eine angemessene Ausstattung der Schulen mit Informationstechnik erarbeitet werden. Die im Rahmen unseres Projektes „Datenschutz an den Schulen in Mecklenburg-Vorpommern“ identifizierten datenschutzrechtlichen Probleme sollen schrittweise gelöst werden. Die Musterschulen sollen dann im weiteren Zeitablauf als Beispiel für die anderen Schulen im Land dienen.

Datenschutzrechtliches Moratorium für die Schulen im Land

Als besonders hohes Risiko für eine datenschutzgerechte Datenverarbeitung an Schulen haben wir die dienstliche Nutzung von privaten Datenverarbeitungsanlagen der Lehrkräfte eingeschätzt.

Nach der Veröffentlichung der Ergebnisse des Projektes „Datenschutz an den Schulen in Mecklenburg-Vorpommern“ im Frühjahr 2016 hat das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern weitere Informationen für die Schulen im Land bereitgestellt. In dem Schreiben des Ministeriums wurden alle Schulen über unser Projekt informiert und die Voraussetzungen für die Nutzung privater Geräte der Lehrkräfte für dienstliche Zwecke erläutert. Diesem Schreiben hatte das Ministerium einen „Antrag für den Gebrauch privater Datenverarbeitungsgeräte zur Verarbeitung personenbezogener Daten von Lehrkräften in Mecklenburg-Vorpommern“ beigefügt, der viele Lehrkräfte erheblich verunsicherte. Uns wurde von Fällen berichtet, in denen Schulleiter den Lehrkräften mit arbeitsrechtlichen Konsequenzen drohten, wenn sie den Antrag nicht unterzeichnen würden. Zahlreiche Schulleiter sowie Lehrkräfte erkundigten sich bei uns, wie sie künftig überhaupt arbeiten sollen, wenn sie die im Vertrag abgebildeten strengen Vorgaben des Schulgesetzes Mecklenburg-Vorpommern und der dazugehörigen Schuldatenschutzverordnung beachten sollen. Wir erklärten daraufhin stets den rechtlichen Sachverhalt und das Ziel des Projektes, zunächst an den Musterschulen die Datenschutzvorgaben umzusetzen und zu testen und die Ergebnisse dann im weiteren Verlauf auf die restlichen Schulen im Land auszuweiten.

Da wir die Verunsicherung an den Schulen jedoch nicht ausräumen konnten, sahen wir uns gezwungen, ein Moratorium für die Schulen im Land zu erlassen. Wir teilten den Schulen mit, dass wir keine verdachtsunabhängigen Kontrollen an den Schulen des Landes bis Juni 2018 durchführen werden. Dies sollte dazu beitragen, praktikable Lösungen für die Zukunft zu finden. Mit dem Schreiben teilten wir aber auch noch einmal die Mindestanforderungen an die Verarbeitung von Daten im schulischen Umfeld mit. Das Schreiben zum Moratorium sowie den Mindestanforderungen war zentraler Inhalt von Schulungen bei der Gewerkschaft Erziehung und Wissenschaft (GEW) sowie dem Verband Bildung und Erziehung (VBE).

6.8.2 Das Schul-Cloud-Projekt des Hasso-Plattner-Instituts

Im Herbst 2016 erfuhren wir aus verschiedenen Veröffentlichungen von den Plänen des Hasso-Plattner-Instituts Potsdam (*HPI*) zur Entwicklung einer sogenannten Schul-Cloud. Die Grundidee dieses Pilotprojektes zur Modernisierung des Schulunterrichts verfolgt den Ansatz, Bildungsinhalte nicht nur in Lehrbüchern oder auf individuellen Rechnern in den Schulen zu platzieren. Stattdessen sollen digitale Lehrinhalte in einer Schul-Cloud zentral auf Servern in Rechenzentren vorgehalten und dadurch überall verfügbar werden. Der Zugriff auf digitale Bildungsangebote und -medien soll somit von jedem Ort aus möglich sein, und in den Schulen würde für derartige Angebote keine eigene, aufwendige und wartungsintensive IT-Infrastruktur mehr erforderlich sein. Zudem soll die Schul-Cloud breite, interaktive Kommunikations- und Kollaborationsmöglichkeiten eröffnen.

So könnten sich Lerngruppen unkompliziert und immer wieder neu auch über große Entfernungen zusammenfinden. Gemeinsame überregionale Bildungsaktionen und -initiativen sind denkbar und leicht zu koordinieren und ein direkter Austausch zwischen Schülerinnen und Schülern, Eltern und Lehrkräften soll ermöglicht werden.

Da wir zu verschiedenen Datenschutzaspekten sowohl im Bereich Cloud, siehe Zwölfter Tätigkeitsbericht, Punkt 4.1.2, als im Bereich Schule, siehe Zwölfter Tätigkeitsbericht, Punkt 2.1, in den letzten Jahren wertvolle Erfahrungen sammeln konnten, die wir gerne in dieses Projekt einfließen lassen wollten, haben wir mit dem HPI Kontakt aufgenommen und unsere Unterstützung angeboten.

Das HPI nahm uns daraufhin in den Fachbeirat des Projektes auf und eröffnete uns somit die Möglichkeit, sehr frühzeitig im Sinne von Data-Protection-by-Design auf die Entwicklung der Schul-Cloud Einfluss zu nehmen. Die Projektverantwortlichen beim HPI hatten sehr früh erkannt, dass die Einhaltung des Datenschutzes eine grundlegende Voraussetzung für jede Digitalisierungsinitiative in deutschen Schulen ist. Es blieb daher auch nicht bei unserer Beteiligung am Projekt. Auf unsere Empfehlung hin wurden auch unsere Kollegen aus Thüringen einbezogen, die den Arbeitskreis Datenschutz und Bildung der Datenschutzkonferenz leiten. Um Datenschutzaspekte gezielt beraten zu können, hat das HPI neben dem Beirat die Taskforce „Datenschutz“ gegründet, in der Kolleginnen und Kollegen aus Datenschutzbehörden weiterer Bundesländer vertreten sind.

Im Ergebnis zahlreicher Gespräche und Treffen - das Projekt wurde beispielsweise auch in einer Sitzung des AK Technik, siehe Punkt 8, vorgestellt und beraten - wurden bereits datenschutzkonforme Lösungen für viele Teilbereiche gefunden und umgesetzt. So läuft die Schul-Cloud bisher ausnahmslos in deutschen Rechenzentren und personenbezogene Daten verlassen in keinem Verarbeitungsschritt Deutschland. Die Cloud basiert auf standardisierten Open-Source-Produkten, was erheblich zur Transparenz des gesamten Verfahrens beiträgt. In die Cloud gelangen nur pseudonymisierte Daten. Anbieter von digitalen Lerninhalten können somit nicht direkt mit Lehrkräften sowie Schülerinnen und Schülern, sondern über die Schul-Cloud nur mit deren pseudonymisierten digitalen Identitäten kommunizieren. Das Pseudonymisierungskonzept wurde Ende 2017 dem AK Technik zur Begutachtung vorgelegt.

Das Schul-Cloud-Projekt befindet sich seit dem Herbst 2017 in der sogenannten Pilotphase und wird an 27 Pilotschulen in 12 Bundesländern, unter anderem in Mecklenburg-Vorpommern, getestet. In enger Abstimmung mit Lehrkräften und Schülerinnen und Schülern werden schrittweise Lerninhalte-Anbieter gewonnen, die ihre digitalen Lernmaterialien über die Cloud zur Verfügung stellen.

Die Schul-Cloud ist ein reines Infrastruktur-Projekt und kein Lerninhalteanbieter. Die teilnehmenden Bundesländer haben die volle Kontrolle darüber, welche Inhalte über die Schul-Cloud angesteuert werden können. Die Schul-Cloud lässt auch weiterhin Raum für landesspezifische Angebote. Zu beachten ist zudem, dass die datenschutzrechtliche Verantwortung für die Nutzung der Cloud bei den teilnehmenden Schulen liegt.

Wir haben deshalb auch mehrfach darauf hingewiesen, dass die Schul-Cloud nicht datenschutzrechtlich legitimiert wird, weil Datenschützer aus Mecklenburg-Vorpommern und Thüringen am Projekt beteiligt sind, und dass durch die Teilnahme von Mitgliedern der Datenschutzkonferenz an dem Projekt keine Bindungswirkung für andere Bundesländer entstehen darf.

Bei der Vorstellung des Projektes in der 93. Datenschutzkonferenz im Frühjahr 2017 haben wir unseren Kolleginnen und Kollegen der anderen Bundesländer empfohlen, sich über die Nutzung der Schul-Cloud in den Pilotschulen ihres Zuständigkeitsbereiches zu informieren und gegebenenfalls weitergehende Empfehlungen auszusprechen. Wir werden das Projekt auch weiterhin gemeinsam mit Kolleginnen und Kollegen anderer Datenschutzaufsichtsbehörden begleiten, um dazu beizutragen, dass die Weiterentwicklung der Schul-Cloud über den Pilotbetrieb hinweg datenschutzgerecht erfolgt.

7 IT-Planungsrat

7.1 Turnusmäßige Sitzungen des IT-Planungsrates

Über den IT-Planungsrat[22] (*IT-PLR*) und die Rolle der Datenschutzaufsichtsbehörden in diesem Gremium haben wir in der Vergangenheit regelmäßig berichtet, zuletzt im Zwölften Tätigkeitsbericht unter Punkt 3. Bereits im Jahr 2010 erteilte uns die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in unserer Eigenschaft als Vorsitzendem des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik, siehe Punkt 8) das Mandat zur Beratung des IT-PLR aus der Sicht der Landesbeauftragten für den Datenschutz.

Nach wie vor vertreten wir die Datenschutzaufsichtsbehörden der Länder im IT-PLR. 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[23] aufmerksam zu machen und andererseits die Datenschutzkonferenz über die Arbeit des IT-PLR zu informieren.

Im folgenden Abschnitt berichten wir über einige Aspekte der Arbeit des IT-PLR, die besonders enge Bezüge zur Tätigkeit der Datenschutzaufsichtsbehörden haben.

7.2 Ausgewählte Aspekte der Tätigkeit des IT-Planungsrates

In seiner 19. Sitzung im März 2016 hat sich der IT-PLR zum wiederholten Mal mit Fragen der Informationssicherheit im Bereich der öffentlichen Verwaltung befasst. Ausgangspunkt war die Leitlinie für Informationssicherheit[24], über die wir bereits im Zwölften Tätigkeitsbericht, siehe dort Punkt 3.3, berichtet hatten.

[22] https://www.it-planungsrat.de/DE/Home/home_node.html
[23] https://www.it-planungsrat.de/DE/Projekte/projekte_node.html
[24] https://www.it-planungsrat.de/DE/Projekte/Steuerungsprojekte/InfoSic/InfoSic_node.html

Schon damals hatten wir die Informationssicherheit in den Kommunen bemängelt und uns dabei auch auf die Ergebnisse unserer Untersuchungen im eigenen Bundesland bezogen, siehe Zwölfter Tätigkeitsbericht, Punkt 2.2.1. Der IT-PLR stellte im März 2016 fest, dass die Leitlinie für Informationssicherheit in der Gesamtschau über den Bund und die Länder zwar zu 74 % umgesetzt sei, nahm aber auch zur Kenntnis, dass ohne zusätzliche Ressourcen die Leitlinie nicht in allen Ländern weiter umgesetzt werden kann. Das würde dazu führen, dass die im Umsetzungsplan beschlossene zeitliche Zielsetzung bis Anfang 2018 unter der Annahme unveränderter Sicherheits-Ressourcen in den Ländern nicht mehr gehalten werden kann. Er bat daraufhin seine Mitglieder, sich dafür einzusetzen, dass die zur Umsetzung notwendigen Ressourcen bereitgestellt werden. Diese Forderung gilt nach wie vor insbesondere auch in Mecklenburg-Vorpommern und insbesondere im kommunalen Bereich und insbesondere dann, wenn Kommunen den Anschluss an das Verbindungsnetz (ehemals DOI) benötigen und dafür die vom IT-Planungsrat am 31. Dezember 2016 beschlossenen „Anschlussbedingungen an das Verbindungsnetz“ erfüllen müssen.

Ebenfalls in der 19. Sitzung hatten wir Gelegenheit, das Standard-Datenschutzmodell (*SDM*), siehe auch Punkt 5.1.1, vorzustellen und über den Stand der Entwicklung zu berichten. Der IT-PLR nahm unseren Bericht zur Kenntnis und begrüßte die Aktivitäten der Datenschutzkonferenz. Er bat seine Mitglieder um Prüfung der damals vorgestellten Version 0.9 und um Rückmeldung gegenüber den Datenschutzbehörden des Bundes und der Länder. Bisher war die Resonanz allerdings gering. Angesichts der steigenden Anforderungen im Bereich des Datenschutzmanagements vor dem Hintergrund der Datenschutz-Grundverordnung, siehe Punkt 3.1, gehen wir jedoch davon aus, dass das SDM in zunehmendem Maße angewendet wird und die Zahl der erbetenen Rückmeldungen steigen wird.

Ein Dauerthema im IT-PLR ist seit der 20. Sitzung im Juni 2016 ein umfassendes Digitalisierungsprogramm für die öffentliche Verwaltung von Bund, Ländern und Kommunen. Technische Basis für dieses Programm sind neben der Digitalisierung der einzelnen Fachverfahren der sogenannte Portalverbund und die Servicekonten für Bürgerinnen und Bürger. Bisher werden Informationen zu Verwaltungsleistungen in der Regel in einem zentralen Landesportal dargestellt. Mit dem Portalverbund soll der Zugang zu Verwaltungsleistungen bundesweit ermöglicht werden. Über Servicekonten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Die 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat im April 2016 in ihrer Entschließung „Datenschutz bei Servicekonten“ Empfehlungen für die datenschutzgerechte Ausgestaltung dieser Servicekonten formuliert [25] . Diese Empfehlungen wurden im Onlinezugangsgesetz (*OZG*) des Bundes weitgehend berücksichtigt. Das 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. Die Planungen des IT-PLR sind mit Ablauf des Berichtszeitraumes noch lange nicht abgeschlossen.

[25] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Entschl_Servicekonten.pdf

Geplant ist, im vom OZG vorgegebenen Zeitraum etwa 500 Verwaltungsdienstleistungen zu digitalisieren. In einem ersten Schritt wurden neun Dienstleistungen identifiziert, die einerseits eine hohe Relevanz für Bürgerinnen und Bürger und andererseits von besonderem Interesse für Unternehmen sind. Im ersten Schritt des Digitalisierungsprogramms sollen sie als sogenannte Leuchtturm-Angebote in den Portalverbund eingebunden werden. Es ist absehbar, dass die datenschutzrechtliche Begleitung des Digitalisierungsprogramms des IT-PLR eine langfristige Aufgabe nicht nur unserer Behörde, sondern aller Datenschutzbehörden von Bund und Ländern sein wird.

8 Arbeitskreis „Technische und organisatorische Datenschutzfragen“

8.1 Turnusmäßige Sitzungen

Über den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (*AK Technik*) der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (*Datenschutzkonferenz*) haben wir in der Vergangenheit regelmäßig berichtet, zuletzt im Zwölften Tätigkeitsbericht unter Punkt 6. Mit Blick auf die von der Europäischen Datenschutz-Grundverordnung (*DS-GVO*) geforderte Pflicht zur Zusammenarbeit der Aufsichtsbehörden (Art. 57 Abs. 1 lit. e, g und Kapitel VII) gewinnt der AK Technik weiter an Bedeutung. Aber auch die Digitalisierung der Verwaltung in Deutschland, siehe Digitalisierungsprogramm des IT-Planungsrates Punkt 7, erfordert eine zunehmende Koordinierung der Aktivitäten der Aufsichtsbehörden im technischen Bereich. Nach wie vor hat die Datenschutzkonferenz uns die Aufgabe übertragen, den AK Technik zu leiten.

Auch in diesem Berichtszeitraum haben wir die bewährte Tagungsfrequenz beibehalten. Wir haben in den Jahren 2016 und 2017 jeweils zwei Sitzungen des AK Technik organisiert und durchgeführt.

Zur **66. Sitzung** im März 2016 hatte die Bundesdatenschutzbeauftragte in ihre Dienststelle nach Bonn eingeladen, um die Mitglieder des AK Technik über den Stand der Beratungen zur DS-GVO zu informieren. Schwerpunkt dieser Sitzung waren die Technikaspekte der DS-GVO und die Möglichkeiten der arbeitsteiligen Bearbeitung der neuen Aufgaben. Ein weiterer Beratungsschwerpunkt betraf die Modernisierung der Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (*BSI*). Gemeinsam mit Vertretern des BSI beriet der AK Technik über die Auswirkungen dieser Modernisierung auf Datenschutzaspekte und über die erforderliche Neujustierung des Verhältnisses von IT-Grundschutz und Datenschutz, insbesondere mit Blick auf das Standard-Datenschutzmodell (*SDM*), siehe Punkt 5.1.1. In dieser Sitzung wurde auch über den Personenbezug von Bildaufnahmen, den Datenschutz im Kraftfahrzeug und die eID-Strategie der Bundesregierung beraten.

Die **67. Sitzung** fand im Oktober 2016 in Schwerin statt. Einen großen Zeitanteil nahm die Diskussion von Datenschutzaspekten beim Einsatz von Produkten der Firma Microsoft ein. Ein Mitarbeiter von Microsoft war als Gast eingeladen und erläuterte den Teilnehmerinnen und Teilnehmern das Konzept der Microsoft-Cloud-Deutschland und Details der neu errichteten Datacenter in Magdeburg und in Frankfurt am Main. Im Laufe der Diskussion wurde deutlich, dass zahlreiche Detailfragen nur im Nachgang zur Sitzung auf Expertenebene geklärt werden können. Es wurde vereinbart, einen ausführlichen Fragenkatalog zu erstellen, dessen Beantwortung Grundlage für weitere Gespräche sein soll. Der Vertreter von Microsoft bot den Mitgliedern des Arbeitskreises an, die Rechenzentren und das dazugehörige Cloud-Control-Center in Berlin zu besichtigen. Dieser Einladung folgten einige Teilnehmerinnen und Teilnehmer im Rahmen eines Workshops des AK Technik im Mai 2017, siehe Punkt 8.2.

Die **68. Sitzung** des Arbeitskreises fand im Februar 2017 auf Einladung des Lehrstuhls Datenschutz und Datensicherheit an der Technischen Universität Dresden statt. Die Wissenschaftler der Universität hatten angeboten, einige ihrer Forschungsprojekte im Bereich Datenschutz vorzustellen. So wurde das Projekt AN.ON-Next, Anonymität Online der nächsten Generation, erläutert, das anonyme Kommunikation im Internet ermöglichen soll. Ein ähnliches Ziel verfolgen weitere Projekte, die die Wissenschaftler unter dem Titel „Mehr Datenschutz mit weniger Aufwand - Leichtgewichte Lösungen für Anwender und Anbieter“ vorstellten. Schließlich wurde mit Blick auf die Steigerung der Effektivität von Prüfungen der Aufsichtsbehörden ein Tool vorgestellt, das die automatisierte Prüfung der Datenschutzkonformität von Webseiten ermöglicht. In einem ersten Praxistest konnte das Tool seine Tauglichkeit nachweisen, indem beim automatisierten Test von 1.893 Webseiten von Land und Kommunen des Freistaates Sachsen zahlreiche gravierende Mängel aufgedeckt wurden. Als Gäste zur Sitzung in Dresden waren auch Vertreter des Arbeitskreises „Organisation und Informationstechnik“ der Rechnungshöfe von Bund und Ländern eingeladen, um die Informationssicherheits-Anforderungen der Rechnungshöfe vorzustellen. Wir konnten zahlreiche Schnittmengen zur Arbeit der Datenschutzaufsichtsbehörden feststellen und vereinbarten die weitere Zusammenarbeit sowie einen Gegenbesuch der Datenschützer im entsprechenden Gremium der Rechnungshöfe.

Die **69. Sitzung** fand im Oktober 2017 in Schwerin statt. Wir hatten erneut Vertreter des Bundesamtes für Sicherheit in der Informationstechnik (*BSI*) eingeladen, um uns diesmal über technische Details der Blockchain-Technologie zu informieren. In einem ersten Meinungsaustausch wurde darüber beraten, ob insbesondere die Gewährleistung von Betroffenenrechten an die Grenzen der Anwendung dieser neuen Technologie stoßen kann. Werden personenbezogene Daten direkt in einer Blockchain gespeichert, ist beispielsweise fraglich, ob die Rechte auf Löschung, Berichtigung oder Sperrung umsetzbar sind. Es wurde herausgearbeitet, dass ein Ausweg die Möglichkeit der Offchaine-Speicherung dieser Daten sein könnte und die Blockchain lediglich als manipulationssicheres Protokoll der Zugriffe auf diese Daten diene. Die Diskussion hat verdeutlicht, dass noch zahlreiche grundlegende Fragen zu klären sind, bis Blockchain-Anwendungen im Kontext personenbezogener Daten im Produktivbetrieb einsetzbar sind.

Als weiterer Gast war ein Mitarbeiter des Hasso-Plattner-Instituts Potsdam (*HPI*) eingeladen, um technische Details des Schul-Cloud-Projektes des HPI vorzustellen und mit den Teilnehmerinnen und Teilnehmern zu beraten, siehe dazu auch Punkt 6.8.2. Besonders großes Interesse zeigte das HPI an der datenschutzrechtlichen Einschätzung des Pseudonymisierungskonzeptes des Projektes durch die Informatiker der Datenschutzbehörden. In der Cloud-Lösung soll sichergestellt werden, dass etwa die Anbieter von digitalen Lehrmaterialien nicht auf personenbezogene Daten der Schülerinnen und Schüler zugreifen können, die online bereitgestellte Lernmaterialien nutzen. Wir haben zugesagt, das Projekt sowohl im entsprechenden Expertengremium als auch im AK Technik auch weiterhin zu beraten.

8.2 Workshop

Wenn spezielle Fragen zum technischen und organisatorischen Datenschutz im Kreis der Datenschutzbeauftragten von Bund und Ländern zu klären sind, an der sowohl Techniker als auch Juristen beteiligt werden, werden spezielle Workshops des AK Technik geplant. Im Juni 2017 haben wir einen solchen Workshop organisiert und durchgeführt. Anlass für diesen Workshop war die von der Firma Microsoft ausgesprochene Einladung zum Besuch des Cloud-Control-Centers in Berlin, siehe Punkt 8.1. Im Cloud-Control-Center wird die Microsoft-Cloud-Deutschland gesteuert und administriert, die die technische Basis für die von Microsoft und T-Systems gemeinsam betriebene Treuhänderlösung darstellt.

Während des Besuches erläuterten Mitarbeiter von Microsoft die vertraglichen Grundlagen der Microsoft-Cloud-Deutschland und gingen auf verschiedene rechtliche Fragen ein. Zudem wurden Compliance-Details und technische Aspekte von Azure-Deutschland erläutert und IT-Sicherheits- und Datenschutzaspekte von Office 365 vorgestellt. Bei der Gelegenheit wurde den Microsoft-Vertretern der ausführliche Fragenkatalog übergeben, der in der 67. Sitzung des AK Technik erbeten worden war. Aber auch dieser Besuch ließ noch zahlreiche Fragen zur Datenschutzkonformität des Treuhändermodells und verschiedener Microsoft-Produkte offen. Deshalb hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder verschiedene Arbeitskreise mit der weiteren Prüfung beauftragt. Eine wesentliche Basis dieser Prüfung sind die Antworten der Firma Microsoft zum oben genannten Fragenkatalog, die uns Ende November 2017 erreicht haben. Die Prüfung ist zum Ende des Berichtszeitraums noch nicht abgeschlossen.

8.3 Technology Subgroup - Zusammenarbeit auf europäischer Ebene

Die Artikel-29-Gruppe wurde als zentrales Koordinierungsgremium für die datenschutzrechtliche Aufsicht innerhalb der Europäischen Union eingerichtet[26]. Ähnlich dem Arbeitskreis Technik, siehe Punkt 8, auf nationaler Ebene dient dabei die „Technology Subgroup“ im internationalen Kontext als Beratungs- und Unterstützungsgremium für die Artikel-29-Gruppe. 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 Technology Subgroup. So ist es uns einerseits möglich, den AK Technik über die laufenden Entwicklungen im europäischen Rahmen zu informieren, und andererseits erlaubt uns die Mitgliedschaft, wichtige nationale Themen und Standpunkte des AK Technik auf internationaler Ebene einzubringen bzw. zu vertreten.

Der regelmäßige Meinungsaustausch und die gemeinsame Meinungsbildung zwischen den europäischen Mitgliedsstaaten werden vor dem Hintergrund der Europäischen Datenschutz-Grundverordnung (*DS-GVO*) massiv an Bedeutung zunehmen. Dazu gehören auch gemeinsame Untersuchungen bei international agierenden Unternehmen wie Microsoft und Google sowie die Erstellung von sogenannten Opinions[27]. In diesen Stellungnahmen - vergleichbar mit den Orientierungshilfen auf nationaler Ebene - werden aktuelle technische und organisatorische Themen aus Datenschutzsicht betrachtet und sowohl rechtlich als auch technisch bewertet. Im Berichtszeitraum wurden dabei unter anderem die Opinions zum Beschäftigtendatenschutz (Data processing at work) (http://ec. europa.eu/newsroom/article29/item-detail.cfm?item_id=610169), zur geplanten ePrivacy-Verordnung (http://ec.europa.eu/newsroom/article29/ item-detail. cfm?item_id=610140) und zu kooperativen intelligenten Verkehrssystemen (Cooperative Intelligent Transport Systems [C-ITS]) (http://ec.europa.eu/newsroom/ just/document.cfm? doc_id=47888) entworfen.

In Vorbereitung der kommenden Datenschutz-Grundverordnung (DS-GVO) werden aber neben den Opinions vermehrt auch Guidelines zu wichtigsten Artikeln erarbeitet. Dabei sind insbesondere die bisher im Berichtszeitraum entstandenen Guidelines zur Datenübertragbarkeit gemäß Art. 20 DS-GVO (http://ec.europa.eu/newsroom/document.cfm?doc_id=45685) und einem FAQ dazu (http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf) sowie zur Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=44137) hervorzuheben.

[26] http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936
[27] http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1308&tpa_id=6936

9 Öffentlichkeitsarbeit

Die Europäische Datenschutz-Grundverordnung (*EU-DSGVO*) enthält in Art. 57 Abs. 1 einen Katalog von 22 Aufgabenfeldern, die die Datenschutzbehörden zu bearbeiten haben. Einige dieser Aufgabenfelder betreffen die Öffentlichkeitsarbeit.

Danach ist es Aufgabe der Datenschutzbehörden, die Öffentlichkeit über datenschutzrechtliche Fragen und Entwicklungen zu informieren, zugleich aber auch die Parlamente und die Regierungen bzw. Verwaltungen zu beraten, die Verantwortlichen und Auftragsverarbeiter für ihre Pflichten zu sensibilisieren und nicht zuletzt auf Anfrage jeder betroffenen Person Informationen über ihre Rechte zu geben. Wir haben also einen umfassenden und differenzierten Informationsauftrag für die Datenschutzbehörden.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat auch in der Vergangenheit bereits sehr umfangreich Öffentlichkeitsarbeit geleistet. Dies ist in diesem Tätigkeitsbericht an verschiedenen Stellen dargelegt. Ein besonderes Augenmerk galt dabei - und wird auch künftig gelten - den Informationen für junge Menschen.

Wir möchten an dieser Stelle allen Partnern, die wir bei dieser Arbeit gehabt haben und mit denen wir zusammengearbeitet haben, herzlich danken. Dieser Dank betrifft insbesondere die Staatskanzlei, die Landesmedienanstalt, das Landeskriminalamt und andere Behörden, aber auch Organisationen der Wirtschaft, wie etwa die Industrie- und Handelskammern.

Trotz all dieser Bemühungen haben wir in der Vergangenheit einen umfassenden Informationsauftrag, wie ihn die Grundverordnung enthält, nicht erfüllt. Wir würden auch in Zukunft erheblich mehr Personal benötigen, um hier wirklich allen Ansprüchen gerecht zu werden. Dies ist umso bedauerlicher, als insbesondere die Medienbildung nicht nur bei jungen Menschen angesichts der wachsenden Bedeutung von Social Media eine absolute Zukunftsaufgabe ist, der mehr Ressourcen zur Verfügung gestellt werden müssten.

10 Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V

Seit nunmehr elf Jahren hat Mecklenburg-Vorpommern ein Informationsfreiheitsgesetz. Es wird zunehmend rege genutzt, die Zahl der Anträge, bei denen wir um Hilfe gebeten werden, steigt stetig. Ebenso wächst die Komplexität der Anfragen. Das Informationsfreiheitsgesetz hat sich als fester Bestandteil von mehr Transparenz und damit mehr direkter Demokratie in Mecklenburg-Vorpommern etabliert. Insofern sind die Zielstellungen des Gesetzgebers - das Gesetz wurde 2006 aus der Mitte des Landtages eingebracht, siehe: Landtagsdrucksache 4/2117 vom 22.02.2006 - zum großen Teil erfüllt worden. Im Vergleich mit den übrigen Bundesländern und dem Bund liegt unser Land einem Transparenzranking zufolge mit einer Punktzahl von 41 genau im Mittelfeld. Zwei Nichtregierungsorganisationen, „Mehr Demokratie e. V.“ und die „Open Knowledge Foundation Deutschland“, hatten zusammen erstmals ein Transparenzranking erstellt und der Öffentlichkeit am 2. März 2017 zugänglich gemacht, www.mehr-demokratie.de/fileadmin/pdf/2017-03-02_Transparenzranking.pdf.

Hamburg erreichte mit seinem fortschrittlichen Transparenzgesetz mit 69 Punkten den ersten Platz. Kriterien für eine positive Bewertung waren unter anderem verbindliche gesetzliche Regelungen von proaktiven Veröffentlichungspflichten, umfassende Auskunftspflichten, eng gefasste Informationsverweigerungsgründe, Länge der Fristen, innerhalb derer Auskunft zu geben ist, und die Höhe der Gebühren.

Auch wenn Mecklenburg-Vorpommern nicht schlecht abschneidet, bedeutet das nicht, dass man die Hände in den Schoß legen kann. Daher haben wir unsere Novellierungsvorschläge für ein modernes Gesetz unter Punkt 10.3 dargestellt.

10.1 Auswirkungen der EU-DSGVO auf die Informationsfreiheit in Mecklenburg-Vorpommern

Am 25. Mai 2016 ist die Europäische Datenschutz-Grundverordnung (EU-DS-GVO) in Kraft getreten. Ab dem 25. Mai 2018 ist sie unmittelbar anwendbar. Das Innenministerium hat uns im Rahmen der Ressortanhörung zum Entwurf eines Gesetzes zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften Mecklenburg-Vorpommerns an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 und eines Gesetzes zur Änderung von Artikel 37 der Verfassung des Landes Mecklenburg-Vorpommern angehört.

Es handelt sich um ein Artikelgesetz, in dessen Artikel 3 Änderungen des § 14 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) formuliert werden. Die Änderungen waren notwendig geworden, da das IFG M-V auf die Befugnisse der bisherigen §§ 29 bis 33 Landesdatenschutzgesetz (DSG M-V) verwies, die ab dem 25. Mai 2018 nicht mehr gelten. Die Artikel 57 und 58 der Verordnung (EU) 2016/679 sehen jedoch weitergehende Rechte für den Datenschutzbeauftragten vor, wie die Verwarnung, die Verhängung von Geldbußen oder Anweisungsbefugnisse, die mit der vermittelnden Funktion des Landesbeauftragten für Informationsfreiheit nicht vereinbar wären. Der Schwerpunkt der Tätigkeit des Informationsfreiheitsbeauftragten liegt in der Beratung der Bürgerinnen und Bürger und der Behörden.

Der Landesbeauftragte für Informationsfreiheit wird in § 14 Abs. 1 des Gesetzentwurfs erstmalig als „Kontrollstelle„ bezeichnet. Schärfstes Mittel bleibt weiterhin die förmliche Beanstandung gegenüber den betreffenden Behörden.

Wir hatten dem Innenministerium in unserer Stellungnahme dazu folgende Empfehlungen bzw. Änderungsvorschläge unterbreitet:

- Die Bezeichnung der Behörde ist mit „Die Landesbeauftragte für Datenschutz und Informationsfreiheit“ oder „Der Landesbeauftragte für Datenschutz und Informationsfreiheit“ vollständig zu benennen Die Kontrollstelle kann das Recht auf Informationsfreiheit zudem nicht „wahren“. Dies ist Aufgabe der Behörden, die den Informationszugang gewährleisten müssen. Die Kontrollstelle kann die Gewährung des Zugangs nur überwachen.

- Zudem haben wir eine andere Reihenfolge der Regelungen angeregt. Diese sollte sich an den „Eskalationsstufen“ bei der Bearbeitung von Petitionen orientieren. Im Vordergrund steht zunächst, dass die Kontrollstelle zunächst immer die öffentliche Stelle zur Stellungnahme auffordert, sich mithin Fragen beantworten lässt bzw. Einsicht in Unterlagen nimmt. Es geht primär um die Beratung und den Ausspruch von Empfehlungen. Eine förmliche Beanstandung ist das letzte Mittel, wenn die Kontrollstelle keine Verständigung zwischen dem Antragsteller und der öffentlichen Stelle bewirken kann. Insofern sollte das Recht zur Beanstandung im Gesetzestext aus systematischen Gründen nach hinten verschoben werden.
- Die Informationsfreiheitsbeauftragten des Bundes und der Länder arbeiten zudem auch eng mit den Informationsfreiheitsbeauftragten der anderen europäischen Mitgliedsstaaten zusammen. Die Zusammenarbeit auf europäischer Ebene sollte daher im Gesetzestext ergänzt werden.
- Es sollte präziser gefasst werden, dass die Kontrollstelle frühzeitig bei dem Entwurf von Gesetzen, die den Informationszugang betreffen, beteiligt wird. Gleiches muss für Verwaltungsvorschriften in einem frühen Entwurfsstadium gelten, insbesondere auch deshalb, weil die Gemeinsame Geschäftsordnung II, Richtlinie zum Erlass von Rechtsvorschriften und weiteren Regelungen durch die Landesregierung (GGO II), für die Informationsfreiheit keine klarstellende Regelung enthält.
- Der vorliegende Entwurf trifft keine Regelungen zum Zweck der Verarbeitung bei Petitionen nach dem Informationsfreiheitsgesetz. Es sollte die Befugnis zur Verarbeitung besonderer Kategorien personenbezogener Daten ergänzt werden.
- Schlussendlich regen wir an, den Berichtszeitraum entsprechend der Regelung im Datenschutzbereich auf ein Jahr zu verkürzen.

Unsere Vorschläge und Empfehlungen ausweislich des Gesetzentwurfs der Landesregierung, Drucksache 7/1568(neu), vom 8. Januar 2018 wurden nicht übernommen. Es erfolgte die Überweisung an den Ausschuss für innere Angelegenheiten und Angelegenheiten der Europäischen Union.

Unsere oben genannten Änderungsvorschläge und Empfehlungen werden wir daher erneut gegenüber dem Landtag vortragen.

10.2 Grundsatzpositionen der Informationsfreiheitsbeauftragten der Länder gegenüber der Bundespolitik

Die Informationsfreiheitsbeauftragten der Länder haben am 6. Oktober 2017 ein Papier zur neuen Legislaturperiode veröffentlicht. Informationen sind die Basis einer Demokratie. Sie sind Grund- und Treibstoff des Prozesses der öffentlichen Meinungsbildung. Transparenz schafft Vertrauen zwischen Politik, Verwaltung und Bevölkerung.

Die Informationsfreiheitsbeauftragten der Länder formulieren zu Beginn der Legislaturperiode fünf Kernforderungen an die Bundespolitik mit dem Ziel, das Transparenz- bzw. Informationsfreiheitsrecht weiterzuentwickeln und seine Akzeptanz zu fördern.

Es sind die Folgenden:

1. Informationsfreiheit in die Verfassungen!
2. Ein Gesetz für den Informationszugang! Hin zu Transparenzgesetzen!
3. Nachrichtendienste ins IFG!
4. Abschaffung unnötiger Ausnahmen!
5. Mehr Transparenz in der Drittmittelforschung!

Die Grundsatzpositionen haben wir auf unserer Webseite [28] veröffentlicht.

10.3 Das Informationsfreiheitsgesetz - weiterer Novellierungsbedarf besteht

Dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern war bewusst, dass das Artikelgesetz zur Anpassung an die Europäische Datenschutz-Grundverordnung (EU-DS-GVO) einem strikten Zeitplan unterlag, da diese bereits ab dem 25. Mai 2018 gilt. Insofern hatten wir im Rahmen der Beteiligung unserer Behörde an dem Gesetzgebungsverfahren auf umfangreiche Änderungsvorschläge zum Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) verzichtet.

Aus Sicht des Informationsfreiheitsbeauftragten ist dieses Gesetz jedoch dringend novellierungsbedürftig. Die Gesetzgebung zur Informationsfreiheit schreitet in fast allen Bundesländern voran. In einigen Ländern existieren bereits weiterentwickelte Transparenzgesetze, wie in Bremen, Hamburg, Rheinland-Pfalz und Baden-Württemberg.

Wir empfehlen auch für Mecklenburg-Vorpommern ein Transparenzgesetz mit klar festgelegten, in einem Transparenzregister zu regelnden Veröffentlichungspflichten. Es reicht nicht aus, dass Informationen nur auf konkreten Antrag hin herausgegeben werden. Vielmehr müssen Informationen aller Behörden, die von öffentlichem Interesse sind, über eine einheitliche Plattform abrufbar sein. Bisher sind wichtige Informationen entweder gar nicht vorhanden oder nur schwer auffindbar. Ein Register kann so funktionieren, dass jede öffentliche Stelle ihre Informationen eigenverantwortlich einstellt. Dies kann beispielsweise durch eine Verlinkung erfolgen. Damit nicht alle öffentlichen Stellen sofort alles an Informationen einstellen müssen, kann man zeitlich vereinbaren, wann was einzustellen ist. Eine derartige Staffelung haben bereits andere Bundesländer gesetzlich geregelt. Eine Überforderung der öffentlichen Stellen mit der Prüfung, was alles in ein Transparenzregister einzugeben wäre, findet somit nicht statt.

[28] https://www.datenschutz-mv.de/informationsfreiheit/publikationen/entschließungen/Grundsatzpostionen

Folgende Informationen sollten in ein solches Register - unter Beachtung der gesetzlich vorgeschriebenen Ausschlusstatbestände - aufgenommen werden:

- Kabinettsbeschlüsse; diese sind zu erläutern, soweit dies für das Verständnis erforderlich ist; Beschlüsse zum Abstimmungsverfahren im Bundesrat sind nur im Ergebnis zu veröffentlichen,
- Berichte und Mitteilungen der Landesregierung an den Landtag,
- Gutachten und Studien, soweit sie von Behörden in Auftrag gegeben wurden, in die Entscheidung der Behörde einfließen oder ihrer Vorbereitung dienen
- in öffentlicher Sitzung gefasste Beschlüsse nebst den dazugehörenden Protokollen und Anlagen,
- die wesentlichen Inhalte von Verträgen von allgemeinem öffentlichen Interesse mit einem Auftragswert von mehr als 20.000,00 EUR, soweit es sich nicht um Beschaffungsverträge handelt,
- Haushalts-, Stellen-, Geschäftsverteilungs- und Aktenpläne,
- Geodaten nach dem Geoinformations- und Vermessungsgesetz Mecklenburg-Vorpommern (GeoVermG M-V)
- die von den transparenzpflichtigen Stellen erstellten öffentlichen Pläne, insbesondere der Landeskrankenhausplan und andere landesweite Planungen
- Zuwendungen, soweit es sich um Fördersummen ab einem Betrag von 1.000,00 EUR handelt
- Zuwendungen an die öffentliche Hand ab einem Betrag von 1.000,00 EUR.

Des Weiteren schlagen wir eine Zusammenlegung von Informationsfreiheitsgesetz (IFG M-V) und Umweltinformationsgesetz (LUIG) vor. Bisher überwachen die Informationsfreiheitsbeauftragten - bis auf wenige Ausnahmen - nur die Einhaltung des allgemeinen Informationsrechts, nicht jedoch die der besonderen Informationszugangsrechte. Eine umfassende Kontroll- und Beratungszuständigkeit, auch für Umweltinformationen, fehlt häufig. Eine solche würde dazu führen, dass Bürgerinnen und Bürger gegen ablehnende Bescheide der öffentlichen Stellen bei Umweltinformationen nicht nur im förmlichen Verfahren (Widerspruch und Klage) vorgehen müssten. Sie könnten sich vielmehr auch an den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden, der dann versucht, den Streit außergerichtlich zu klären. Dies erspart den Antragstellern und den Behörden Kosten und Zeit.

Eine Zusammenlegung der beiden Gesetze würde auch dazu führen, dass der Schutz von Betriebs- und Geschäftsgeheimnissen einer Abwägung mit dem öffentlichen Interesse unterläge. Wenn das öffentliche Interesse überwiegt, sind die Informationen herauszugeben. Dies ist schon jetzt so im Bereich des Umweltrechts in § 9 Abs. 1 Nr. 3 Umweltinformationsgesetz (UIG) geregelt, der auf § 3 LUIG verweist.

Schlussendlich halten wir eine Regelung zur elektronischen Antragstellung einschließlich der Erhebung von Gebühren für zeitgemäß.

10.4 Frühzeitige Herausgabe von Informationen über Meistbietenden

Ein Bürger informierte uns darüber, dass er bei einer Stadt einen Antrag gestellt habe auf Zugang zu Informationen, die im Zusammenhang stehen mit einer öffentlichen Ausschreibung der Vergabe eines Erbbaurechts und dem Verkauf der auf dem Grundstück aufstehenden Gebäude gegen Höchstgebot. Dies hatte die Stadt jedoch abgelehnt.

Die Stadtvertretung hatte in einer Sitzung im Ergebnis der Ausschreibung die Vergabe eines Erbbaurechtes an dieser Fläche und den Verkauf der auf ihr aufstehenden Gebäude an den Meistbietenden beschlossen. Des Weiteren hatte die Stadt dem Antragsteller mitgeteilt, dass ein Vertrag mit dem Meistbietenden noch nicht geschlossen worden sei. Trotzdem wollte der Antragsteller schon zu diesem Zeitpunkt, als der Vertrag mit dem derzeit Meistbietenden noch nicht geschlossen war, die Höhe des erzielten Erbbauzinses und die Höhe des Kaufpreises wissen. Er war der Auffassung, dass ein Antrag auf Zugang zu Informationen nur dann abzulehnen sei, wenn durch die vorzeitige Bekanntgabe der Erfolg der Entscheidung vereitelt würde. Dies sei offensichtlich nicht der Fall.

Wir haben die Rechtslage aus informationsfreiheitsrechtlicher Sicht wie folgt beurteilt:

Gemäß § 6 Abs. 1 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) ist der Antrag auf Zugang zu Informationen abzulehnen für Entwürfe zu Entscheidungen sowie die Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung, soweit und solange durch die vorzeitige Bekanntgabe der Informationen der Erfolg der Entscheidung vereitelt würde. Hier kommt der Beschluss der Stadtvertretung zur unmittelbaren Vorbereitung einer Entscheidung in Betracht. Die Entscheidung bestand darin, an den Meistbietenden zu verkaufen. Wenn nun der aus der Ausschreibung ermittelte Meistbietende den Vertrag nicht unterschreibt und die Informationen zur Höhe des erzielten Erbbauzinses und zur Höhe des Kaufpreises aufgrund des Informationsfreiheitsantrags des Antragstellers herausgegeben werden würden, könnte dieser sich in einer möglichen zweiten Ausschreibung an dem Gebot des bisher „Meistbietenden“ orientieren. Intention der Stadt ist es jedoch, auch bei einer zweiten Ausschreibung den höchstmöglichen Gewinn zu erzielen. Insofern besteht in der Tat aus Sicht der Stadt die Gefahr, dass durch die vorzeitige Bekanntgabe der betreffenden Informationen der Erfolg der Entscheidung vereitelt würde.

Ebenso ist der Antrag auf Informationszugang nach § 6 Abs. 6 IFG M-V abzulehnen, wenn zu befürchten ist, dass durch das Bekanntwerden der Informationen der Erfolg behördlicher Maßnahmen gefährdet oder vereitelt sowie die ordnungsgemäße Erfüllung der Aufgaben der betroffenen Behörde erheblich beeinträchtigt würde. Behördliche Maßnahmen wären hier die Ausschreibung und möglicherweise - abhängig davon, ob der Meistbietende unterschreibt - eine zweite Ausschreibung. Der „Erfolg“ der Maßnahme(n) wäre hier im konkreten Fall ein möglichst hoher zu erzielender Gewinn für die Stadt. Dieser Erfolg könnte gefährdet sein, wenn die Beträge zum Erbbauzins und zum Kaufpreis bereits frühzeitig bekannt werden. Nach dem Gesetzestext reicht die Befürchtung, dass dies eintritt, aus. Die Kommunen sind nach haushaltsrechtlichen Grundsätzen zu einer wirtschaftlichen Haushaltsführung verpflichtet. Eine solche gehört auch zur „ordnungsgemäßen Erfüllung der Aufgaben der betroffenen Behörde“.

Zudem hatte die Stadt dem Antragsteller zugesichert, dass ihm nach wirksamer Beurkundung des sich in der Verhandlung befindlichen Vertrages die entsprechenden Informationen herausgegeben werden würden. Insofern war die Argumentation der Stadt nicht zu beanstanden.

10.5 Verweigerung der Herausgabe eines Pachtvertrages an Ferienhauseigentümerin

Ein Rechtsvertreter hat uns im Namen seiner Mandantin gemäß § 14 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) um Vermittlung gebeten. Die Mandantin begehrte als Ferienhauseigentümerin die Übersendung der Kopie eines Pachtvertrages, welcher zwischen einer Verpächterin und einem eingetragenen Verein (e. V.) geschlossen worden ist. In dem Vertrag waren Einzelheiten über den Stegbereich und die Unterhaltung des Steges am Ufergelände getroffen worden. Danach gingen die Pflege und Erhaltung des Steges zulasten des Vereins, der die entsprechenden Kosten den Liegeplatznutzern auferlegen wollte. Der Antragstellerin kam es darauf an, sich Klarheit darüber zu verschaffen, ob und in welchem Umfang sie zu den Kosten herangezogen werden würde. Der Pächter wollte ihr keine Einsicht gewähren. Die Verpächterin, bei der die Antragstellerin einen förmlichen IFG-Antrag gestellt hatte, hatte ihr zunächst einen ablehnenden Bescheid übermittelt, woraufhin sie Widerspruch einlegte.

Wir haben die Rechtslage aus informationsfreiheitsrechtlicher Sicht wie folgt beurteilt:

Grundsätzlich hat die Antragstellerin ein Recht auf Zugang zu den bei den Behörden vorhandenen Informationen, es sei denn, es greifen die Ausschlusstatbestände der §§ 5 bis 8 IFG M-V. Hier kam § 7 Nr. 5 IFG M-V in Betracht. Die Verpächterin hatte im Rahmen des Beteiligungsverfahrens (§ 9 IFG M-V) den Vereinsvorsitzenden eingeschaltet und dieser hatte die Informationsgewährung abgelehnt. Gemäß § 7 Nr. 5 IFG M-V ist der Antrag auf Informationen abzulehnen, soweit durch das Bekanntwerden der Informationen personenbezogene Daten offenbart werden, es sei denn, der Antragsteller macht ein rechtliches Interesse an der Kenntnis der begehrten Informationen geltend. Ein rechtliches Interesse liegt (auch) dann vor, wenn der Informationszugang möglicherweise größere Klarheit über den Sach- und Streitstand vermittelt und aus Sicht eines verständigen Betrachters die weitere Rechtsverfolgung oder -verteidigung erleichtert wird. Der Antragstellerin kam es ersichtlich darauf an zu wissen, ob und in welcher Höhe sie sich als Hauseigentümerin an den Kosten, die dem Verein entstehen, beteiligen muss. Sie wollte sich Klarheit verschaffen und aus diesem Grund den Pachtvertrag einsehen. Insofern ist ein rechtliches Interesse gegeben. Des Weiteren setzt § 7 Nr. 5 IFG M-V voraus, dass überwiegende schutzwürdige Belange des Betroffenen einer Offenbarung nicht entgegenstehen. Als Betroffener kommt der Vereinsvorsitzende in Betracht. Dieser dürfte den Pachtvertrag im Namen des Vereins unterschrieben haben. Inwiefern mutmaßlich die Unterschrift im Namen des Vereins „überwiegende schutzwürdige Belange“ darstellen, die einer Übersendung des Pachtvertrages entgegenstehen, ist nicht ersichtlich. Hierzu ist auch nichts dargelegt worden.

Daher war auch die Begründung des Vereinsvorsitzenden, dass der Ferienhauseigentümerin keine Kosten entstehen, irrelevant. Diese muss sich nicht auf mündliche Angaben des Vereinsvorsitzenden verlassen. Vielmehr hat sie einen Anspruch auf Einsichtnahme in den Pachtvertrag.

Nach nochmaliger Prüfung der Sach- und Rechtslage hat die Verpächterin den Bescheid aufgehoben und die gewünschten Informationen herausgegeben.

10.6 Transparenz beim NDR

Die Vergangenheit hat gezeigt, dass der Norddeutsche Rundfunk (NDR) sich nicht sehr auskunftsfreudig gezeigt hat, was Anträge nach den jeweiligen Transparenz- bzw. Informationsfreiheitsgesetzen der Länder Hamburg, Schleswig-Holstein und Mecklenburg-Vorpommern betrifft.

Die meisten Anfragen, gerade auch solche, die über die Plattform FragDenStaat.de gestellt wurden, wurden nur nach Belieben bzw. gar nicht beantwortet. Das liegt daran, dass der NDR der Auffassung ist, dass er gesetzlich nicht zur Auskunft verpflichtet sei. Bei dem NDR handelt es sich bekanntlich um eine Vier-Länder-Anstalt. Die Regierungen der vier Länder, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein führen die Rechtsaufsicht über den NDR im Wechsel von jeweils 18 Monaten. Zwar könnte man hinsichtlich der rechtlichen Regelungen auf das Sitzland abstellen. Aber selbst eine solche Regelung ist rechtlich nicht zwingend. Die Entscheidung darüber, welches Recht anwendbar ist, müssen die Länder gemeinsam treffen. Einem Land allein fehlt die Gesetzgebungszuständigkeit.

Regelungsstandort kann der NDR-Staatsvertrag sein, der alle vier Vertragsländer bindet. Hier sollte eine Regelung getroffen werden, die den NDR zur Herausgabe von Informationen verpflichtet, unabhängig davon, ob ein Informationsfreiheitsantrag in Schwerin, Kiel oder Hamburg gestellt wird.

Die Staatskanzlei unseres Landes hat zwischenzeitlich signalisiert, dass sich die Chefs der norddeutschen Staats- und Senatskanzleien darüber einig seien, dass eine Klarstellung bzw. feste Regelung zur Informationsfreiheit und Transparenz im NDR-Staatsvertrag sinnvoll sei.

Wie genau diese Regelung aussehen wird, bleibt abzuwarten.

10.7 Anwendbarkeit des IFG nach Abschluss des Vergabeverfahrens im Unterschwellenbereich

Ein Antragsteller hatte uns um Vermittlung hinsichtlich eines Antrags nach dem Informationsfreiheitsgesetz gebeten. Inhaltlich ging es um Vergaberecht. Er hatte eine Hochschule aufgefordert, ihm sowohl die eingereichten Bewerbungsunterlagen aller Mitbewerber für eine Dienstleistungskonzession als auch das Protokoll der Angebotseröffnung in Kopie zur Verfügung zu stellen.

Die Vergabedokumentation, also das Protokoll der Angebotseröffnung, wurde ihm übermittelt. Im Hinblick auf die Übersendung der Bewerbungsunterlagen der anderen Mitbewerber äußerte die Hochschule rechtliche Bedenken. Sie vertrat die Auffassung, dass § 4 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) in Konkurrenz stehe zu § 7 und § 8 IFG M-V. So enthielten die Angebote zum einen personenbezogene Daten, für deren Offenbarung nicht die datenschutzrechtlich erforderliche Einwilligung der Betroffenen vorliege, und zum anderen würden durch die Übermittlung der unternehmensbezogenen Tatsachen Betriebs- und Geschäftsgeheimnisse offenbart, in die die Betroffenen nicht eingewilligt hätten.

Wir haben dazu folgende Auffassung vertreten:

Es dürfte unstreitig sein, dass nach Abschluss des Vergabeverfahrens im Unterschwellenbereich (Auftragswert für Liefer- und Dienstleistungen unter 10.000 Euro) das IFG M-V grundsätzlich anwendbar ist. Die Ausschlusstatbestände, insbesondere die von der Hochschule bereits angeführten §§ 7, 8 i. V. m. § 9 sind grundsätzlich zu prüfen. Insbesondere wäre hier im Zusammenhang mit Kalkulationen von Mitbewerbern zu prüfen gewesen, ob ein Informationszugang die Wettbewerbsposition des betreffenden Unternehmers nachteilig beeinflussen würde. So müsste ein Unternehmer, auch der, der den Zuschlag erhalten hat, darlegen, dass durch eine Offenlegung der Informationen, also der Kalkulation seines Angebots, seine Wettbewerbsposition beeinträchtigt würde.

Die Beurteilung der Wettbewerbsrelevanz einer betrieblichen oder geschäftlichen Information erfordert mitunter eine wertende Einschätzung der öffentlichen Stelle. So wäre beispielsweise eine Wettbewerbsrelevanz gegeben, wenn die Hochschule jedes Jahr gleiche oder ähnlich gelagerte Vergaben für derartige Veranstaltungen durchführt. In einem solchen Fall könnte der Antragsteller aus Kalkulationen von Mitbewerbern möglicherweise anhand der Kalkulation desjenigen Mitbewerbers, der den Zuschlag erhalten hat, nachvollziehen, wie er seine eigene Kalkulation für die nächste Veranstaltung so berechnet, dass er gerade noch unter dem Angebot des günstigsten Bewerbers liegt. Wenn die Vergabe der Bewertungskonzession jedoch von Jahr zu Jahr immer anders ausgeschrieben wird, könnte der Antragsteller aus den für 2017 vorliegenden Kalkulationen der Mitbewerber keine Rückschlüsse ziehen. Somit würde insbesondere dem Mitbewerber, der den Zuschlag erhalten hat, kein Wettbewerbsnachteil für ein künftiges Vergabeverfahren entstehen.

Die Hochschule argumentierte, dass der Anwendung des § 1 Abs. 1 IFG M-V im vorliegenden Fall die Sperrwirkung des § 1 Abs. 3 IFG M-V entgegenstehe und zitiert dazu entsprechende Rechtsprechung des Bundesverwaltungsgerichts. Dabei übersieht sie jedoch, dass die Vorschrift im Bundesrecht viel restriktiver ist als die in unserem Landesrecht. Demnach besteht hier eine Anspruchskonkurrenz. Es sind grundsätzlich die Ansprüche nach dem speziellen Gesetz und die nach dem IFG M-V zu prüfen.

Letztlich stellte sich heraus, dass der geschätzte Auftragswert der Dienstleistungskonzession den Schwellenwert für die Anwendung des Vergabegesetzes von 10.000 Euro weit überschritt. Ebenso legte die Hochschule dar, dass die Dienstleistungskonzession für die Bewirtung jährlich wiederkehrend zu vergleichbaren Wettbewerbsbedingungen vergeben wird. Insofern hätte der Antragsteller, würden die Kalkulationsunterlagen der anderen Mitbewerber einschließlich desjenigen, der den Zuschlag erhalten hat, herausgegeben, einen Wettbewerbsvorteil.

Insofern war hier im Ergebnis der Anspruch auf Informationszugang abzulehnen.

10.8 Bauvorlagen als Betriebs- oder Geschäftsgeheimnisse

Ein Antragsteller hatte mich gemäß § 14 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) um Unterstützung gebeten. Er trug vor, dass er Räumlichkeiten und das gesamte Inventar in einem Gebäude übernommen habe. In diesen Räumen sei zuvor eine Diskothek betrieben worden. Er beabsichtige, dort ebenfalls Musikveranstaltungen durchzuführen. Er habe daher beim Gewerbeamt beantragt, die Erlaubnis für eine Schank- und Speisewirtschaft mit regelmäßigen Musik- und Tanzveranstaltungen einschließlich Terrassenversorgung zu erhalten. Im Rahmen eines Erlaubnisverfahrens habe das Bauamt die Ansicht vertreten, für eine derartige Nutzung der Räumlichkeiten sei ein Antrag auf Nutzungsänderung zu stellen. Der Antragsteller verlangte daraufhin, Akteneinsicht in die ursprüngliche Baugenehmigungsakte zu erhalten. Nachdem ein formloser Antrag zunächst abgelehnt worden war, hat er nochmals einen förmlichen Antrag nach § 1 Abs. 2 IFG M-V gestellt. Dieser Antrag war von der Stadt in Form eines Bescheides abgelehnt worden. Dagegen hat der Antragsteller Widerspruch eingelegt.

Wir haben uns dazu wie folgt geäußert:

Grundsätzlich hat jede natürliche und juristische Person des Privatrechts Anspruch auf Zugang zu den bei einer Behörde vorhandenen Informationen. Der Antrag auf Zugang zu Informationen darf nur dann verweigert werden, wenn einer der Ausschlusstatbestände der §§ 5 bis 7 IFG M-V in Betracht kommt. Die Stadt berief sich auf § 7 IFG M-V. Gemäß § 7 S. 1 Nr. 1 IFG M-V ist der Antrag auf Zugang zu Informationen abzulehnen, soweit durch das Bekanntwerden der Informationen personenbezogene Daten offenbart werden, es sei denn, die Betroffenen willigen ein. § 7 dient dem verfassungsrechtlich in Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 Grundgesetz (GG) verankerten Recht auf informationelle Selbstbestimmung. Dieser Schutz ist bei natürlichen Personen höher zu werten als der einfachgesetzliche Informationszugangsanspruch. Im vorliegenden Fall handelte es sich jedoch um eine juristische Person des Privatrechts und zudem noch um eine 100%ige Tochter der Stadt, sodass diese sich nicht auf § 7 IFG M-V berufen konnte.

Des Weiteren trug die Stadt vor, dass der Informationszugang nach § 8 IFG M-V abzulehnen wäre, da der Grundstückseigentümer gleichzeitig auch der Entwurfsverfasser der Bauvorlagen sei, in die Akteneinsicht begehrt werde und auf deren Grundlage ein eigener Nutzungsänderungsvertrag gestellt werden soll.

Hier stünden der Schutz geistigen Eigentums und der Schutz von Betriebs- und Geschäftsgeheimnissen entgegen. Der Betroffene habe nicht eingewilligt. Hierzu ist zu sagen, dass allein die Behauptung des Vorliegens nicht ausreicht. In Betracht käme hier allenfalls eine Beeinträchtigung des Urheberrechts in Form von Verwertungsrechten. Dies erfordert

- eine persönliche Schöpfung des Urhebers
- einen geistigen Gehalt,
- eine wahrnehmbare Formgestaltung und
- eine in der Schöpfung zum Ausdruck kommende Individualität des Urhebers, also eine gewisse Gestaltungshöhe.

Insbesondere an letzterem Punkt scheitern die meisten zu schützenden Werke. Die Darstellung muss in schöpferischer Weise vom Herkömmlichen abweichen und über das rein Handwerksmäßige hinausgehen. Im konkreten Fall war nichts dargelegt worden, dass die in Rede stehenden Bauvorlagen diese Gestaltungshöhe erreichen und mithin geistiges Eigentum darstellen. Insofern gab es keinen Grund, den Informationszugang zu verweigern.

Ebenso war nicht erkennbar, dass Betriebs- und Geschäftsgeheimnisse i. S. d. § 8 S. 1 IFG M-V einschlägig sind, die zu einem Beteiligungsverfahren i. S. d. § 9 IFG M-V führen müssten. Als Betriebs- und Geschäftsgeheimnisse werden allgemein alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat, so das Bundesverfassungsgericht (BVerfG), Beschluss vom 14. März 2006 - 1 BvR 2007, 2111/03. Ein solches Wissen fehlt, wenn die Offenlegung der Information nicht geeignet ist, exklusives technisches oder kaufmännisches Wissen an Marktkonkurrenten zugänglich zu machen oder so die Wettbewerbsposition des Unternehmens nachhaltig zu beeinflussen.

Die Entscheidung darüber, ob im konkreten Fall ein Betriebs- und Geschäftsgeheimnis anzuerkennen ist, obliegt allein der mit dem Informationszugang befassten Behörde. Wir kamen zu der Einschätzung, dass im vorliegenden Fall die hier in Rede stehenden Bauvorlagen weder ein Betriebs- noch ein Geschäftsgeheimnis darstellten. Selbst wenn derartige Geheimnisse vorliegen, kann die Behörde immer noch dem Antrag in dem Umfang stattgeben, in dem der Informationszugang ohne Preisgabe der geheimhaltungsbedürftigen Informationen möglich ist.
Die Stadt hat uns daraufhin mitgeteilt, dass sie unserer Rechtsauffassung folgen und dem Antrag auf Akteneinsicht stattgeben werde. Das anhängige Widerspruchsverfahren wurde eingestellt.

11 Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder
AO	Abgabenordnung
BÄO M-V	Berufsordnung für die Ärztinnen und Ärzte in M-V
BDSG	Bundesdatenschutzgesetz
BDSGnF	Bundesdatenschutzgesetz neue Fassung
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BKAG	Bundeskriminalamtgesetz
BMeldDÜV	Datenübermittlungen der Meldebehörden
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
CSG	ComputerSpielSchule Greifswald
CMS	Content-Management-System
CN-LAVINE	Corporate Network der Landesverwaltung
DDoS	verteilte (engl. distributed) Denial of Service
DES	Data Encryption Standard
DNS	Domain Name Systems
DOI	Deutschland Online Infrastruktur e. V.
DRK	Deutsches Rotes Kreuz
DSAnpUG-EU	Datenschutz-Anpassungs- und Umsetzungsgesetz EU
DSFA	Datenschutz-Folgenabschätzung
DSGV	Deutsche Sparkassen- und Giroverband
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
eAkte	elektronische Akte
EDV	elektronische Datenverarbeitung
EG	europäische Gemeinschaft
eGo-MV	Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern
eID	elektronischer Identitätsnachweis
EU	Europäische Union
FTP	File Transport Protocol
GeoVermG M-V	Geoinformations- und Vermessungsgesetz Mecklenburg-Vorpommern
GEZ	Gebühreneinzugszentrale
GEW	Gewerkschaft Erziehung und Wissenschaft
GG	Grundgesetz
GKR	gemeinsames Krebsregister der neuen Bundesländer und Berlin
HPI	Hasso-Plattner-Institut Potsdam

HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
ID	Identifikationsnummer
IFG M-V	Informationsfreiheitsgesetz Mecklenburg-Vorpommern
IMK	Innenministerkonferenz
IDEV	Internet-Datenerhebung im Verbund
IoT	Internet of Things (engl. Internet der Dinge)
IP	Internet Protocol
IPsec	Internet Protocol Security
IT-PLR	IT-Planungsrat
IQMV	Institut für Qualitätsmanagement Mecklenburg-Vorpommern
Jfn	Jugend fragt nach
JiL	Jugend im Landtag
JVA	Justizvollzugsanstalt
Kfz	Kraftfahrzeug
KITA	Kindertagesstätte
KlinKrebsRG	Klinisches Krebsregistergesetz
KommSt	Kommunikationsinfrastruktur für die Landesverwaltung
KoSIT	Koordinierungsstelle für IT Standards
KRG	Gesetz über Krebsregister
KrebsRG M-V	Krebsregistrierungsgesetz Mecklenburg-Vorpommern
LAKOST	Landeskoordinierungsstelle für Suchtvorbeugung
LGVB	länderübergreifende gebündelte Verfahrensbetreuung
LJR M-V	Landesjugendring Mecklenburg-Vorpommern
LKA	Landeskriminalamt
LMG	Landesmeldegesetz
LT-Drs.	Landtags-Drucksache
LuftVZO	Luftverkehrs-Zulassungs-Ordnung
LUIG	Landes- Umweltinformationsgesetz
MDM	Mobile Device Management
MRZ	Machine Readable Zone
NDR	Norddeutscher Rundfunk
nPA	neuer Personalausweis
OpenPGP	Open Pretty Good Privacy
OSCI	Online Services Computer Interface
OWiG	Gesetz über Ordnungswidrigkeiten
OVG M-V	Oberverwaltungsgericht Mecklenburg-Vorpommern
OZG	Onlinezugangsgesetz
PAS	Patientenaktensysteme
PassG	Passgesetz
PAuswG	Personalausweisgesetz
PDF	Portable Document Format - plattformunabhängiges Dateiformat für Dokumente
PersVG M-V	Personalvertretungsgesetz Mecklenburg-Vorpommern
PFS	perfect forward secrecy
PIA	Privacy Impact Assessment
QES	qualifizierte elektronische Signatur
RFID	Radio-Frequency Identification
RIS	Ratsinformationssystem

SchulDSVO M-V	Schuldatenschutzverordnung Mecklenburg-Vorpommern
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SDM	Standard-Datenschutzmodell
SGB I	Sozialgesetzbuch Erstes Buch
SGB II	Sozialgesetzbuch Zweites Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SGB XII	Sozialgesetzbuch Zwölftes Buch
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
SSL	Secure Sockets Layer
SMTP	Simple Mail Transfer Protocol
SOG	Sicherheits- und Ordnungsgesetz
StGB	Strafgesetzbuch
StVG	Straßenverkehrsgesetz
TR	Technische Richtlinie
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TEO	Tage ethischer Orientierung
TLS	Transport Layer Security
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.
TMG	Telemediengesetz
UIG	Umweltinformationsgesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
VBE	Verband Bildung und Erziehung
vdek e. V.	Verband der Ersatzkassen e. V.
VDI	Virtual Desktop Infrastructure
VerpflG	Verpflichtungsgesetz
VPN	Virtual Private Network
VwVfG	Verwaltungsverfahrensgesetz
VZÄ	Vollzeitäquivalenten
WWW	World Wide Web
ZIR	zentrales Informationsregister
ZKKR	zentrales Klinisches Krebsregister

12 Stichwortverzeichnis

Diese digitale Selbstverteidigung.....32
Abgabenordnung.....89
AG Digitale Schule.....92
AK Technik.....45, 95, 97, 100, 103
Akteneinsicht.....117
Algorithmen.....18
AN.ON-Next.....101
Angebotseröffnung.....115
Antrag.....111
Antragsteller.....111
Apps.....50
Arbeitsgruppe KITA.....40
Arbeitskreis Datenschutz und Bildung....95
Arbeitskreis Technische und organisatorische Datenschutzfragen.....97, 100
Artikel 57 Ziffer 1b.....32
Artikelgesetz.....107
Auditierung.....49
Auftragsverarbeitung.....90
Auskunft.....67, 106
Auskunftsrecht.....67
Ausstattung der Aufsichtsbehörde.....27
automatisierte Entscheidungen.....55
Azure.....103
Bankverbindungen.....83
Bauamt.....116
Baugenehmigungsakte.....117
Bauvorlagen.....117
BDSGnF.....21
Beanstandung.....107
Behördlicher Datenschutzbeauftragter....92
Belastbarkeit.....76
Beratung.....107
Berechtigungskonzept.....75
Beschäftigtendatenschutz.....103
Bescheid.....114
Beteiligungsverfahren.....113
Betriebs- und Geschäftsgeheimnis.....115
Betriebs- und Geschäftsgeheimnisse.....111
Bewerbungsunterlagen.....115
Big Data.....18, 55
Bildung in der digitalen Welt.....32
Bildungsmaßnahmen.....30
Blockchain.....101
BMI.....17
Brandschutz.....62
Browser.....58
BSI.....46
BSI-Grundschutzmethodik.....100
BSI-Standard.....46
Bundesamt für Sicherheit in der Informationstechnik.....46, 53
Bundesdatenschutzbeauftragte.....17
Bundesdatenschutzgesetz.....17
Bundesinnenminister.....17
Bundesministerium des Inneren.....17
Bundesministerium des Innern.....17
Bürgerbegehren.....81
Bußgelder.....23
Cloud.....94
Cloud Control Center.....101
CMS.....26
Compliance.....23
Computerspielschule Greifswald.....35
Content Management System.....26, 119
DANE.....57
Data-Protection by Design.....95
Datenminimierung.....45
Datenportabilität.....22
Datenreichtum.....20
Datenschutz an den Schulen in Mecklenburg-Vorpommern.....91
Datenschutzfolgenabschätzung.22, 76, 104
Datenschutz-Folgenabschätzung....47, 119
Datenschutzgrundverordnung.....30
Datenschutz-Grundverordnung..15, 17, 24, 45, 98, 100, 104
Datenschutzkonferenz.....15, 20, 96
Datenschutzmanagement.....98
Datensicherheit.....51, 75
Datensparsamkeit.....13, 50, 57
Datenübertragbarkeit.....104
Datenverarbeitung im Auftrag.....90
Demokratie.....106, 108
den Dialog mit Politik.....38
der Medienbildung.....32
der modularen Fortbildung.....42
Dienstanweisung.....77
Dienstvereinbarung.....77
digitale Identität.....95
digitale Lehrinhalte.....94
digitale Signatur.....78
Digitalisierung.....19, 33, 49, 53, 100
Digitalisierungsprogramm.....100
Digitalisierungsproramm.....98
Diskothek.....116
Diskriminierung.....19
DNS.....58
DNSSEC.....58

DOMEA 53
Drittmittelforschung 109
DRK 60
Drohne 60, 61
DSFA 47
DS-GVO 24, 45, 100
E-Government 10, 48
E-Government-Gesetz 53
eID-Strategie 100
Einkommens- und Vermögenssituation ..84
Einwilligung 82, 84, 115
Einwohnerantrag 81
Einwohnerbeteiligung 81
Elterngespräche 43
Ende-zu-Ende-Verschlüsselung 10, 25
ePrivacy Verordnung 104
Erzieher*innen 33
EU-Datenschutzgrundverordnung 106
Europäische Datenschutz-Grundverordnung 18
Europäischer Datenschutzausschuss 16
Europäischer Datenschutztag 18
Fachverfahren 48
Falldatei Rauschgift 16
Feuerwehr 62
Finanzausschuss 27
Finanzbehörde 89
Finanzministerium 89, 90
Finanzverwaltung 90
FragDenStaat.de 114
Friedhof 82
frühkindlichen Bereich 35
Gebühren 106
Gesetzgebung 109
Gesundheits-App 16
GEW 94
Gewährleistungsziel 45
Gewerbeamt 116
Graffiti 64
Grundrechtseingriff 46
Grundsatzpositionen 109
Grundschutzmethodik 46
Halterabfrage 69
Hasso-Plattner-Institut 94
Hasso-Plattner-Instituts Potsdam 102
Haushaltsplan 28
Hausrecht 64
Hochschule 115
HPI 94, 102
IDEV 57
IFG-Antrag 113
IMK 17
informationelle Selbstbestimmung 65
Informationen 108
Informationsfreiheit 114
Informationsfreiheitsgesetz .. 106, 109, 112, 115
Informationsfreiheitsrecht 109
Informationssicherheit 97
Informationszugang 108, 112, 117
Infrastruktur 48, 52
Innenministerium 107
Innenministerkonferenz 17
Integrität 45, 54, 75, 76
Internet 59, 74
Intervenierbarkeit 45
IT-Grundschutz 100
IT-Grundschutz-Kompendium 46
IT-Planungsrat 16, 25, 48, 49, 97, 100
IT-Planungsrates 100
IT-PLR 25, 97
Jugend fragt nach 34
Jugend im Landtag 34
Kalkulation 116
Kamera 62
Kameras 64
Klage 111
KommSt 2017 24
Kommunalverfassung 81
Kommunikationssicherheit 48
Komplexität 106
Konferenz der unabhängigen Daten-schutzbehörden des Bundes und der Länder 24
Kontaktgruppe 17
Kontrollstelle 107
Kooperationsveinbarung 33
Kooperationsvereinbarung zur Medienkompetenzförderung 39
Kopie 113
KoSIT 48
Kraftfahrzeugbundesamt 69
Kühlungsborner Erklärung 16
Kultusministerkonferenz 32
künstliche Intelligenz 18
Landesbeauftragten für Informationsfreiheit 107
Landesdatenschutzgesetz 30

Landesdatenschutzrecht 22
Landesjugendring 35
Landeskoordinierungsstelle für Suchtthemen 35
Landeskriminalamt 35
Landesrechnungshof 23, 27
lebensWerte Gesellschaft 33
Legislaturperiode 108
Lehrkräfte 93
Leitlinie für Informationssicherheit 97
Luftverkehrsordnung 60
Medienaktiv 37
Medienaktiv meets Politik 38
Medienaneignung, ...43
Medienangebot 38
Medienanstalt 35
Medienbildung 33
Medienerlebnissen 43
Medienkompetenzförderung 32
Mediennutzung 43
medienpädagogische Angebote 43
medienpädagogischen Einrichtung 39
Medienpolitische Forderungen 38
Medienscouts MV 35
Medienzentrum Greifswald e. V. 35
Meistbietenden 111
Microsoft 101
Microsoft Cloud Deutschland 101
Mikrozensus 57
Mitbewerber 115
Mitwirkungspflicht 83
mobiles Endgerät 26
Moratorium 93, 94
Musterschulen 92
Nachvollziehbarkeit 57
NDR 114
NDR-Staatsvertrag 114
Nichtverkettung 45
Norddeutsche Rundfunk 114
Notfallplan 11
Nutzung 41
Offchaine-Speicherung 102
Offenbarung 90
öffentliche Ausschreibung 111
Office 365 103
Öffnungsklausel 21
Onlinezugangsgesetz 98
Open-Source 95
Organisationsuntersuchung 28
OSCI-Transport 48
Pachtvertrag 113
Parkplatz 68
Patch 48
Patientendokumentation 88
Patientengeheimnis, ...88
People Score 19
Personalausweis 90
Plakatkampagne 41
Plakatmotiv 41
Plattform 114
Portalverbund 16, 98
Predictive Policing 20
Privatsphäre 19, 33
Profiling 19
Projektbericht 91
Protokoll 115
Protokollierung 54, 77
Pseudonymisierung 95
Pseudonymisierungskonzept 102
Ratsinformationssysteme 74, 122
Rechnungshof 101
rechtliches Interesse 113
Rettungscopter 60
Rettungsschwimmer 60
Risiko 46
Risikoanalyse 76
Schlüsselkompetenz 39
Schrotthändler 90
Schul-Cloud 94
Schul-Cloud-Projekt 102
Schulgesetz 91
Schulhöfe 65
Schutz geistigen Eigentums 117
Schutz von Betriebs- und Geschäftsgeheimnissen 117
Schutzbedarf 46
Schwellenwert 116
SDM 45
SDM-Newsletter 47
Servicekonto 16, 98
Sicherheitskonzept 76
Sicherheitslücke 48
Smart City 50
Smart Home 50
Smartphone 26, 49, 50, 59
Sonderkonferenz 17
soziale Netzwerke 19, 49
Sozialleistungen 83

Staatskanzlei 114
Staatsvertrag 90
Stadtvertretung 111
Standard-Datenschutzmodell 45, 98, 100
Statistisches Amt 57
Steuerdaten 90
Steuergeheimnis 90
Steuerpflichtige 89
Support 90
Tablet 26, 49, 59, 74
technische und organisatorische Maßnahmen 75
Thin Client 25
TLS 57
TLSA/DANE 57
Transparenz 45, 57, 106, 109, 114
Transparenzgesetz 106, 109
Transparenzranking 106
Transparenzregister 109
Traueranzeige 82
Treuhänderlösung 102
TSLA 57
Überwachung 19
Umweltinformation 111
Umweltinformationsgesetz 111
unabhängigen, neutralen und vernetzenden Stelle 38
Unabhängigkeit 16, 28
Unterschriftenliste 81
Unterschwellenbereich 115
Vandalismus 64
VBE 94
Verantwortung 48
Verbindungsnetz 98
Verein 113
Verfügbarkeit 45, 54, 76
Vergabedokumentation 115
Vergaberecht 115
Vergabeverfahren 115
Veröffentlichungspflicht 106, 109
Verpächterin 113
Verschlüsselung 10, 78
Verstehen 41
Vertraulichkeit 45, 54, 75, 76
Videokonferenz 25
Videokonferenzanlage 25
Videoüberwachung 17, 63, 65
Videoüberwachungs-Verbesserungsgesetz 16
Vier-Länder-Anstalt 114
Virtual Desktop Infrastructure 25
Virtualisierung 52
Virtualisierungstechnik 25
Vorbildfunktion 42
Wearables 16
Webbrowser 58
webdays 34
Webseite des Landesbeauftragten 26
Webseitendesign 26
Weiterbildungsreihe 42
Werbewiderspruch 67
Wettbewerbsrelevanz 115
Widerspruch 111, 113, 117
Wirkungsweise 41
XTA 48
XTA 2 49
Zertifikat 57
Zertifizierungsstelle 57
Zertifizierungsverfahren 47
Zielstellung 106
Zugang zu Informationen 111, 117
Zwangsgeld 67
Zweckbindung 55