LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 7/6311**
7. Wahlperiode **21.07.2021**

UNTERRICHTUNG

durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Sechzehnter Tätigkeitsbericht zum Datenschutz

Berichtszeitraum: 1. Januar 2020 bis 31. Dezember 2020

Zugeleitet mit Schreiben des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern vom 16. Juli 2021

Vorwort

Mit den nachfolgenden Ausführungen lege ich den gemäß Artikel 59 Europäische Datenschutz-Grundverordnung (DS-GVO) geforderten Jahresbericht dem Landtag, der Landesregierung und der Öffentlichkeit vor. Der Berichtszeitraum umfasst das Kalenderjahr 2020.

Heinz Müller
Landesbeauftragter für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern

Inhaltsverzeichnis

Seite

Seite

0 Empfehlungen

0.1 Zusammenfassung aller Empfehlungen

1. Das neue Bundesdatenschutzgesetz (BDSG) sieht vor, dass der Bundesrat als Stellvertreter einen Leiter der Aufsichtsbehörde eines Landes wählt. Das ist bislang jedoch nicht geschehen. Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass dies schnellstmöglich nachgeholt wird, *siehe Punkt 3.1*.
2. Wir wiederholen unsere Empfehlung aus dem 15. Tätigkeitsbericht an die Landesregierung, sich dafür einzusetzen, dass bei der Modernisierung der Verwaltungsregister der verfassungskonforme Architekturansatz bereichsspezifischer Identifier beispielsweise in Anlehnung an das österreichische Stammzahlensystem umgesetzt wird und keine einheitlichen und verwaltungsübergreifenden Personenkennzeichen gebildet werden. Wir fordern die Landesregierung auf, im Bundesrat dem Entwurf des Registermodernisierungsgesetzes nicht zuzustimmen, *siehe Punkt 4.3.2*.
3. Wir empfehlen der Landesregierung, bei der Digitalisierung von Verwaltungsdienstleistungen im Rahmen des Einer-für-alle-Prinzips frühzeitig die datenschutzrechtlichen Rahmenbedingungen zu berücksichtigen, das Beratungsangebot der Datenschutzkonferenz in Anspruch zu nehmen und uns frühzeitig in die Entwicklung der digitalen Angebote einzubeziehen, *siehe Punkt 4.3.3*.
4. Wir empfehlen der Landesregierung, sowohl bei der Umsetzung des Onlinezugangsgesetzes (OZG) als auch bei der Weiterentwicklung der gesamten IT-Infrastruktur des Landes die Prinzipien der Digitalen Souveränität zu berücksichtigen. Dies erfordert eine umfassende, moderne IT-Strategie, die zu einer weitgehenden Unabhängigkeit von einzelnen Herstellern führen muss. Von der Entwicklung des Standardarbeitsplatzes im Rahmen des Projektes „MV-PC“ über die Erarbeitung neuer Strukturen für die E-Akte bis hin zu strategischen Überlegungen hinsichtlich der gesamten IT-Infrastruktur des Landes muss das Thema „Open Source“ eine zentrale Rolle spielen, *siehe Punkt 4.3.4*.
5. Wir empfehlen den Verantwortlichen in Wirtschaft und Verwaltung, bei der Auswahl und beim Betrieb von Videokonferenzsystemen die Empfehlungen der „Orientierungshilfe Videokonferenzsysteme“ zu berücksichtigen, *siehe Punkt 5.1*.
6. Wir empfehlen der Landesregierung bei der Gestaltung künftiger Regelungen in Bezug auf die Corona-Pandemie, die bisherigen Erfahrungen und Probleme bei der Umsetzung datenschutzrechtlicher Belange in den Blick zu nehmen, sodass die Kommunen auch die Verantwortlichen und Betreiber von Einrichtungen und Sportstätten angemessen unterstützen können, *siehe Punkt 5.5*.
7. Wir empfehlen, dass die Polizei bei der Überprüfung von Ausweisdokumenten künftig keine Fotos der Ausweise anfertigen sollte, *siehe Punkt 5.6*.
8. Wir empfehlen der Landesregierung, die Vermittlung von Medienkompetenz/Digitaler Kompetenz entlang der gesamten Bildungskette prioritär zu behandeln, um allen Bürgerinnen und Bürgern die Teilhabe an unserer digitalen Kultur zu ermöglichen, *siehe Punkt 6.1*.
9. Nach wie vor aktuell ist unsere Empfehlung an die Landesregierung, bei der Einrichtung und beim Betrieb von personenbezogenen Verarbeitungstätigkeiten die im Standard-Datenschutz-Modell (SDM) beschriebene Vorgehensweise anzuwenden und das dort beschriebene Datenschutz-Management-System einzurichten, *siehe Punkt 7.1*.

10. Wir empfehlen den Verantwortlichen sowohl im öffentlichen als auch im nicht-öffentlichen Bereich, die Onlinedienste von Microsoft (z. B. die Bürosoftware Microsoft Office 365 mit Word, Excel, PowerPoint) im Rahmen der Auftragsverarbeitung bereits einsetzen oder deren Einsatz planen, zu prüfen, ob sie in der Lage sind, diese Produkte datenschutzgerecht einzusetzen. Prüfmaßstab sind die Arbeitsergebnisse des Arbeitskreises Verwaltung der Datenschutzkonferenz. Insbesondere mit Blick auf die Anforderungen zur Gewährleistung der Digitalen Souveränität empfehlen wir den Verantwortlichen den Einsatz alternativer Produkte, insbesondere aus dem Open Source Bereich, zu prüfen, *siehe Punkt 7.2*.
11. Wir empfehlen der Landesregierung, PC-Arbeitsplätze künftig nur mit solchen Betriebssystemen auszustatten, die eine rechtmäßige Verarbeitung personenbezogener Daten erlauben (Art. 6 DS-GVO) und die es ermöglichen, die Grundsätze für die Verarbeitung personenbezogener Daten zu gewährleisten (Art. 5 DS-GVO). Bestehende PC-Arbeitsplätze müssen mittelfristig angepasst werden, *siehe Punkt 7.3*.
12. Wir empfehlen der Landesregierung, den Einsatz dem Stand der Technik entsprechender Verschlüsselungslösungen zu fördern und dem Bestreben, solche Lösungen zu schwächen, entschieden entgegenzutreten, *siehe Punkt 8.1.2*.
13. Wir empfehlen der Landesregierung, uns bei der Erfüllung unseres gesetzlichen Auftrages wie erforderlich zu unterstützen, *siehe Punkt 8.4.1*.
14. Wir empfehlen dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, den Austausch mit unserer Behörde zum ISY-Projekt weiter fortzuführen. Zudem empfehlen wir dem Ministerium, uns im Sinne vertrauensvoller Zusammenarbeit auch künftig frühzeitig in neue Projekte mit Bezug zu datenschutzrechtlichen Grundsatzfragen einzubinden, *siehe Punkt 8.5.1*.

0.2 Umsetzung der Empfehlungen des Fünfzehnten Tätigkeitsberichtes

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 15. TB
1	Das neue Bundesdatenschutzgesetz (BDSG) sieht vor, dass der Bundesrat als Stellvertreter einen Leiter der Aufsichtsbehörde eines Landes wählt. Das ist bislang jedoch nicht geschehen. Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass dies schnellstmöglich nachgeholt wird.	Mit Ablauf des Berichtszeitraumes war der Stellvertreter noch immer nicht gewählt.	4.1.1
2	Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass bei der Modernisierung der Verwaltungsregister der verfassungskonforme Architekturansatz bereichsspezifischer Identifier in Anlehnung an das österreichische Stammzahlensystem umgesetzt wird und keine einheitlichen und verwaltungsübergreifenden Personenkennzeichen gebildet werden.	Mit Ablauf des Berichtszeitraumes hat die Landesregierung mitgeteilt, dass ihr die Position der Datenschutzkonferenz bekannt ist. Sie teilt jedoch die Sichtweise des Bundes, dass bereichsspezifische Identifikationsnummern in keinem vertretbaren Verhältnis zwischen Aufwand und Nutzen zueinanderstehen würden. Somit befürwortet die Landesregierung unsere Empfehlung nicht und hat sich	5.3.2

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 15. TB
		somit nicht für einen verfassungskonformen Architekturansatz eingesetzt.	
3.	Wir empfehlen Verantwortlichen in Wirtschaft und Verwaltung, vor dem Einsatz von Verfahren zur Verarbeitung biometrischer Daten zu prüfen, ob die Verarbeitung die Zulässigkeitsvoraussetzungen des Artikels 6 DS-GVO erfüllt und ob die zusätzlichen, strengeren Voraussetzungen des Artikels 9 DS-GVO eingehalten werden können, und dabei die Empfehlungen des Positionspapiers „Biometrische Analyse“ zu berücksichtigen.	Die Landesregierung hat die Empfehlungen bezüglich des datenschutzkonformen Einsatzes von Verfahren zur Verarbeitung biometrischer Daten zur Kenntnis genommen. Sie hat zugesagt, schon vor der Einführung von Prozessen unter Verwendung von biometrischen Daten die zusätzlichen Anforderungen der DS-GVO in einem Datenschutz- und Sicherheitskonzept verpflichtend mit aufzunehmen.	7.1.1
4.	Wir empfehlen den Verantwortlichen, genau zu prüfen, ob sie die beim Einsatz von Windows 10 entstehenden Risiken beherrschen können. Falls nicht, sollten andere Betriebssysteme, insbesondere aus dem Open Source Bereich, in Betracht gezogen werden.	Die Landesregierung hat zugesagt, das Prüfschema der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Einhaltung des Datenschutzes bei Windows 10 anzuwenden. Ihrer Ansicht nach konnte mit dessen Anwendung sowie mit Hilfe von vorhandenen technischen und organisatorischen Möglichkeiten, der Umsetzung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und einer eigenverantwortlichen Risikoabschätzung der Einsatz von Windows 10 ermöglicht werden.	7.1.2
5.	Wir empfehlen der Landesregierung, bereits bei den Planungen zum Einsatz von KI-Systemen die damit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sorgfältig zu analysieren und die Risiken beim Betrieb derartiger Systeme durch technische und organisatorische Maßnahmen auf ein verantwortbares Maß zu reduzieren.	Die Landesregierung hat uns mitgeteilt, dass sich derzeitig keine KI- bzw. KI-gestützten Systeme im Einsatz oder in der Planung befinden. Sollten diese zukünftig in Betracht gezogen werden, sollen datenschutzrechtliche Anforderungen frühzeitig berücksichtigt werden.	7.1.3
6.	Wir empfehlen den Verantwortlichen in Wirtschaft und Verwaltung, entweder die Einführung von Microsoft Office365 solange zurückzustellen, bis die rechtlichen Rahmenbedingungen geklärt sind, oder den Einsatz anderer	Die Landesregierung hat uns mitgeteilt, dass für die Überprüfung der Kompatibilität zu Produkten aus dem Open Source Bereich umfangreiche Recherchen erforderlich sind.	7.1.4

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 15. TB
	Produkte, insbesondere aus dem Open Source Bereich, zu prüfen.	Die Landesregierung hat jedoch eine Prüfung zugesagt, inwieweit Lösungen implementiert werden können, die eine gemeinsame Datenhaltung möglich machen. Ein Prüfergebnis liegt uns zum Ende des Berichtszeitraumes jedoch nicht vor.	
7.	Wir wiederholen unsere Empfehlung an die Landesregierung aus dem Vierzehnten Tätigkeitsbericht, bei der Einrichtung und beim Betrieb von personenbezogenen Verarbeitungstätigkeiten die im Standard-Datenschutz-Modell (SDM) beschriebene Vorgehensweise anzuwenden und das dort beschriebene Datenschutz-Management-System einzurichten.	Die Landesregierung hat uns mitgeteilt, dass das Standard-Datenschutz-Modell zukünftig in Abstimmung mit uns in den Prozessen der Landesregierung berücksichtigt werden soll.	7.1.5
8.	Wir wiederholen unsere Empfehlung aus dem Vierzehnten Tätigkeitsbericht, die erforderlichen Rechtsgrundlagen für die Einrichtung und Registrierung von Nutzerkonten zu schaffen und die datenschutzrechtlichen Verantwortlichkeiten zwischen den am Verfahren Beteiligten zu klären. Bis zum Inkrafttreten des Zweiten Gesetzes zur Änderung des E-Government-Gesetzes und dem Erlassen der vorgesehenen Rechtsverordnung empfehlen wir eine Übergangsregelung, etwa einen Kabinettsbeschluss.	Die notwendigen Rechtsgrundlagen für die Einrichtung und Registrierung von Nutzerkonten bestanden zum Ende des Berichtszeitraumes immer noch nicht vollständig. Das entsprechende Gesetzgebungsverfahren zur Änderung des E-Government-Gesetzes Mecklenburg-Vorpommern (EGovG M-V) war zwar abgeschlossen. Es fehlt aber die erforderliche Rechtsverordnung der Landesregierung gemäß § 15 dieses Gesetzes.	7.1.6
9.	Wir empfehlen Verantwortlichen in Wirtschaft und Verwaltung, ein geeignetes Passwortmanagement aufzubauen und es einem regelmäßigen Revisionsprozess zu unterwerfen. Bei bereits vorhandenem Passwortmanagement sollte geprüft werden, ob es dem Stand der Technik entspricht.	Die Landesregierung hat uns zugesagt, dass sie interne Sicherheitsmaßnahmen sehr ernst nehmen und die Einführung beziehungsweise Betreuung eines geeigneten Passwortmanagementsystems prüfen wird. Zudem werden die Beschäftigten hinsichtlich der IT-Sicherheitsthemen regelmäßig sensibilisiert und es werden Schulungen angeboten.	7.1.8
10.	Wir empfehlen Verantwortlichen, sich frühzeitig mit dem Thema Zertifizierung vertraut zu machen. Zertifikate bieten das Potenzial, sich bei Verarbeitungsvorgängen (etwa bei Auftragsverarbeitung oder Cloudstrukturen) Klarheit darüber zu verschaffen, ob die	Die Landesregierung hat uns mitgeteilt, dass sie die Empfehlung, sich mit Zertifizierungen vertraut zu machen, zur Kenntnis nimmt. Ferner beschäftigt sie sich bereits mit	7.2

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 15. TB
	gesetzlichen Datenschutzanforderungen eingehalten werden.	dem Potenzial von Zertifizierungen hinsichtlich Auftragsverarbeitung und Cloudstrukturen sowie deren Implementation.	
11.	Wir empfehlen den Verantwortlichen in Krankenhäusern, bei Planungen und beim Betrieb von Messenger-Diensten die Anregungen des Whitepapers „Technische Anforderungen an Messenger-Dienste im Krankenhaus“ zu berücksichtigen und sich an der Diskussion zur Weiterentwicklung des Papiers zu beteiligen.	Die Landesregierung hat diesen Bericht einschließlich des Whitepapers an die Krankenhausgesellschaft Mecklenburg-Vorpommern weitergeleitet, verbunden mit der Anregung, ihrerseits die Mitglieder zu informieren, da sich die Empfehlungen zu Messenger-Diensten an die Verantwortlichen in Krankhäusern richten.	7.3.1
12.	Wir empfehlen den Webseitenanbietern in unserem Bundesland, ihre Webseiten an die vorgenannten neuen Regeln anzupassen. Dies gilt insbesondere für das Einbinden von Dritt-Inhalten und gilt auch für Tracking-Mechanismen. Wer Funktionen nutzt, die eine informierte Einwilligung erfordern, muss entweder eine informierte Einwilligung einholen oder die Funktion entfernen.	Die Landesregierung hat uns mitgeteilt zu prüfen, ob ein weiterer Handlungsbedarf für die von der Landesregierung betriebenen Internetseiten besteht. Ein Prüfergebnis liegt uns zum Ende des Berichtszeitraumes jedoch nicht vor.	7.3.2
13.	Wir empfehlen Verantwortlichen, einen festen Prozess zu etablieren und Beschäftigte entsprechend zu schulen, wie mit Betroffenenrechten umzugehen ist.	Die Empfehlung ist offenbar noch nicht vollständig umgesetzt.	8.1.4
14.	Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass die Planungen zum stetigen Meldedatenabgleich für den Rundfunkbeitrag eingestellt werden.	Die Landesregierung weist unsere Bedenken und die der Datenschutzkonferenz zurück. Wir halten unsere Empfehlung aufrecht.	8.1.6
15.	Wir empfehlen dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, den sehr produktiven Meinungsaustausch mit uns beizubehalten, die Abstände der Gespräche zwischen beiden Häusern im Jahr 2020 jedoch deutlich zu verkürzen.	Der Empfehlung wurde gefolgt.	8.8.1

1 Zahlen und Fakten

Die Tatsache, dass die Europäische Datenschutz-Grundverordnung (DS-GVO) im Berichtszeitraum schon geraume Zeit gültig war, hat zu einer Veränderung der Aufgabenzusammensetzung, insgesamt aber nicht zu einem Rückgang des Aufgabenvolumens geführt, sondern wir können eine weitere Ausweitung feststellen. Das zentrale Ereignis des Jahres 2020, die Corona-Pandemie, hat allerdings massive Auswirkungen auf Aufgabenstruktur und Aufgabenvolumen der Behörde gehabt. Hier ging es auf der einen Seite um unmittelbare Fragen im Zusammenhang mit Corona, zum Beispiel die datenschutzrechtliche Zulässigkeit von Besucherlisten in Restaurants und ähnliches, auf der anderen Seite aber auch um durch die Corona-Pandemie verstärkte Entwicklungen, wie etwa die massiv verstärkte Nutzung von Videokonferenzsystemen, bei denen sich in zunehmendem Umfang die Frage nach ihrer Datenschutzkonformität stellte.
Während im Jahr 2019 noch 175 Veranstaltungen stattfanden, waren dies im Jahr 2020 nur noch 27. Die Maßnahmen zur Pandemieeindämmung, die unter anderem eine drastische Reduzierung unmittelbarer Kontakte vorsahen, führten dazu, dass viele Veranstaltungen ausfallen mussten, insbesondere auch im Bereich unserer Medienbildung. Wir haben es zum Beispiel als sehr schmerzlich empfunden, dass die „Medienscouts MV“-Wochenenden für Jugendliche ausfallen mussten. Andere Veranstaltungen wurden aufgrund der äußeren Rahmenbedingungen gar nicht erst geplant.
Lag die Zahl der Maßnahmen nach Art. 58 Abs. 2 DS-GVO noch bei 82, so waren es im Berichtszeitraum bereits 105. In einer ganzen Reihe von Fällen wurden Maßnahmen lediglich angedroht, aber letztlich nicht vollzogen, da die Androhung bereits die gewünschte Wirkung entfaltete. Unter den 105 Fällen befinden sich auch fünf Fälle, in denen wir eine Geldbuße verhängt haben. Darüber hinaus wurden in zwei Fällen Zwangsgelder festgesetzt sowie zwei Bußgelder auf einer anderen Rechtsgrundlage verhängt.
Im Berichtszeitraum wurden uns von den Verantwortlichen gemäß Art. 33 DS-GVO 173 Datenpannen gemeldet (Vorjahr: 108). Hier ist also ebenfalls ein sehr deutlicher Zuwachs festzustellen. Die Zahl der Eingaben und Beschwerden ist von 533 im Jahr 2019 auf 790 im Jahr 2020 gestiegen. Die Stellungnahmen, Empfehlungen, Beratungen und Prüfanfragen - hier waren 2019 793 Fälle zu verzeichnen - summierten sich im Berichtszeitraum auf 1 524 Fälle. Darüber hinaus wurden 66 vom Parlament oder von der Regierung angeforderte Beratungen durchgeführt.
Die Zahl der anlassbezogenen Prüfungen (aufgrund von Anfragen, Meldungen, Beschwerden etc.) ist von 67 im Jahre 2019 auf 134 im Berichtszeitraum stark gestiegen. Die Zahl der anlassunabhängigen Kontrollen, bei denen wir als Behörde festlegen, wo wir eine Kontrolle vornehmen, verharrt mit fünf (Vorjahr: drei) auf einem extrem niedrigen Niveau, obwohl gerade hier eine große Möglichkeit besteht, tatsächlich Datenschutz zu stärken.
Die Zahl der europäischen Verfahren, unter anderem Kohärenzverfahren nach Art. 67 DS-GVO, bei denen es in 2019 einen leichten Rückgang auf 1 069 Fälle gegeben hat, ist mit 1 350 Fällen wieder deutlich angestiegen.
Insgesamt zeigen diese Zahlen überdeutlich, dass sich die Aufgaben zwar in ihrer Struktur etwas verändert haben, in ihrem Volumen - von einem sehr hohen Niveau kommend - aber nicht etwa kleiner, sondern deutlich größer geworden sind. Der Glaube an eine „Aufgabenblase“ durch die DS-GVO hat sich also auch im Berichtszeitraum als kapitaler Irrtum erwiesen.

2 Entwicklung der Behörde

Das weiter angewachsene Aufgabenvolumen musste durch unsere Behörde mit einer unveränderten Stellenzahl bewältigt werden. Die im Haushalt vorgesehenen Stellen wurden nicht entsperrt, sondern der Landtag verharrte in seiner Blockadehaltung. Lediglich bei einer Hebung, bei der wir im Jahr 2020 eine Klage vorbereitet haben, konnte in 2021 eine Entsperrung erreicht werden.
Da eine Erhöhung der Stellenzahl nicht möglich war, haben wir mit den zur Verfügung stehenden haushaltsrechtlichen Möglichkeiten versucht, das Aufgabenvolumen irgendwie zu bewältigen. Insbesondere wurde der Titel für Aushilfskräfte genutzt, um temporäre Verbesserungen zu finanzieren. Daueraufgaben werden also mit Aushilfskräften erfüllt.
Diese Situation führt für die Bürgerinnen und Bürger, die sich an uns wenden, leider immer häufiger zu Unmut, da wir beispielsweise in aller Regel nicht in der Lage sind, Eingangsbestätigungen für Eingaben und Beschwerden verschicken zu können, und die Bearbeitungszeiten sehr häufig lang sind. Die in der Landesverfassung garantierten Grundrechte sind an dieser Stelle also durchaus in Gefahr.
Die Corona-Pandemie führte in unserer Behörde zu einer Veränderung der Aufgabenstruktur, siehe Punkt 1, aber auch zu einer Veränderung der Arbeitsweise. Zeitweise hat die Behörde komplett im Home-Office gearbeitet, zeitweise wurde ein Zweischichtensystem etabliert. Viele der Aktivitäten der Behörde sind über Videokonferenzen organisiert worden; dies bezieht sich insbesondere auf die Abstimmung mit den Behörden in anderen Bundesländern und den notwendigen fachlichen Austausch in der Datenschutzkonferenz und ihren Arbeitskreisen, aber auch auf die Kommunikation innerhalb der Behörde. Dieses war nicht kurzfristig technisch umzusetzen, sondern benötigte einen gewissen Vorlauf. Die Datenschutzaufsichtsbehörden haben hierzu auch eine Orientierungshilfe erarbeitet, siehe Punkt 5.1.
Zum eigenen Gebrauch und um selbst Erfahrungen im Umgang mit solchen Systemen zu sammeln, haben wir ein eigenes Videokonferenzsystem aufgesetzt. Unsere Wahl fiel dabei auf die Open-Source-Lösung BigBlueButton, die wir auf einem gemieteten Server eines deutschen Anbieters installiert haben. Auf diese Weise konnten wir eine Lösung realisieren, die den Anforderungen des Datenschutzes gerecht wird. Die Sicherstellung der Verfügbarkeit des Systems stellte uns allerdings vor Herausforderungen, da das System auf Dauer qualifiziert gepflegt und administriert werden muss und unsere personellen Ressourcen beschränkt sind. Im kommenden Berichtszeitraum wird uns dieses Thema deshalb weiter begleiten.
Dies, aber auch grundsätzliche Probleme des Home-Office, haben an einigen Punkten zu Qualitätsverlusten in der Arbeit geführt. Beispielsweise kommen Akten der Staatsanwaltschaften grundsätzlich in Papierform zu uns, was bedeutet, dass zumindest zur Entgegennahme der Unterlagen jemand in der Behörde sein muss. Veranstaltungen fielen weitgehend aus, Weiterbildung musste digital organisiert werden.

3 Zusammenarbeit auf europäischer Ebene

3.1 Europäischer Datenschutzausschuss (EDSA)

Der Europäische Datenschutzausschuss (EDSA) besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern. Deutschland wird im EDSA durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vertreten. Das Bundesdatenschutzgesetz (BDSG) sieht vor, dass der Bundesrat als Stellvertreter einen Leiter der Aufsichtsbehörde eines Landes wählt. Das ist jedoch seit 2018 nicht geschehen.

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

- Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen
- Übermittlung personenbezogener Daten zwischen EWR- und Nicht-EWR-Behörden und -Einrichtungen
- Verarbeitung von Gesundheitsdaten zum Zwecke der wissenschaftlichen Forschung im Zusammenhang mit dem COVID-19-Ausbruch
- Verwendung von Standortdaten und Verfahren zur Ermittlung von Kontaktpersonen im Zusammenhang mit dem COVID-19-Ausbruch
- Einwilligung nach der Verordnung 2016/679
- Verhältnis der Zweiten Zahlungsdiensterichtlinie und der DS-GVO
- Die Begriffe „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO
- Die gezielte Ansprache von Social-Media-Nutzern
- Maßgebliche und begründete Einsprüche nach der Verordnung 2016/679

veröffentlicht. Die Erarbeitung dieser Leitlinien erfolgt in Arbeitsgruppen, sogenannten Subgroups, die aus Mitarbeiterinnen und Mitarbeitern der Aufsichtsbehörden der Mitgliedstaaten bestehen. Soweit es uns zeitlich möglich ist, beteiligen wir uns an der Erarbeitung solcher Leitlinien. Zudem waren wir bis August 2020 als ständiger Vertreter der deutschen Landesdatenschutzbeauftragten Mitglied der Technology Subgroup und entsenden bei Bedarf ein stellvertretendes Mitglied in die Enforcement Subgroup.

Das neue Bundesdatenschutzgesetz (BDSG) sieht vor, dass der Bundesrat als Stellvertreter einen Leiter der Aufsichtsbehörde eines Landes wählt. Das ist bislang jedoch nicht geschehen. Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass dies schnellstmöglich nachgeholt wird.

3.2 Enforcement Subgroup

Die Enforcement Subgroup, eine Arbeitsgruppe des Europäischen Datenschutzausschusses (EDSA), befasst sich mit praktischen Fragen der Durchsetzung der Europäischen Datenschutz-Grundverordnung (DS-GVO). Die Vertretung der Landesdatenschutzbeauftragten in der Enforcement Subgroup nehmen die Kollegen der Landesbeauftragten für Datenschutz und Informationsfreiheit Niedersachsen wahr, im Vertretungsfalle wir. Die Sitzungen der Enforcement Subgroup finden normalerweise etwa alle zwei Monate in Brüssel statt. Wegen der COVID-19-Pandemie kam die Subgroup im Berichtszeitraum nur im Februar in Brüssel zusammen, 15 weitere Sitzungen fanden in Form von Videokonferenzen statt.

Inhaltlich hat sich die Enforcement Subgroup als Forum für den Erfahrungsaustausch und die Klärung von Rechtsfragen anhand von Fallbeispielen aus der Praxis etabliert. Darüber hinaus wurden in der Enforcement Subgroup im Berichtszeitraum hauptsächlich die Leitlinie über den maßgeblichen und begründeten Einspruch gegen den Entscheidungsentwurf der federführenden Aufsichtsbehörde und der Entwurf für die erste verbindliche Entscheidung des EDSA in einem Streitbeilegungsverfahren nach Art. 65 Abs. 1 DS-GVO erarbeitet.
Nach den Vorschriften über die Zusammenarbeit der europäischen Aufsichtsbehörden hat die federführende Aufsichtsbehörde den anderen betroffenen Aufsichtsbehörden unverzüglich einen Beschlussentwurf zur Stellungnahme vorzulegen. Gegen diesen Beschlussentwurf kann jede der betroffenen Aufsichtsbehörden innerhalb eines Monats einen maßgeblichen und begründeten Einspruch einlegen. Welche Anforderungen ein maßgeblicher und begründeter Einspruch zu erfüllen hat, bedurfte der Klarstellung. Die Leitlinie über den maßgeblichen und begründeten Einspruch macht deutlich, dass die betroffene Aufsichtsbehörde in ihrem Einspruch begründet darlegen muss, inwieweit sie bei der Frage, ob ein Verstoß gegen die DS-GVO vorliegt oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen zulässig ist, zu einem anderen Ergebnis kommt als die federführende Aufsichtsbehörde und welche Risiken von dem Beschlussentwurf mit Blick auf die Grundrechte und Grundfreiheiten der betroffenen Personen ausgehen. Schließt sich die federführende Aufsichtsbehörde dem maßgeblichen und begründeten Einspruch nicht an oder ist sie der Ansicht, dass der Einspruch nicht maßgeblich oder nicht begründet ist, leitet sie das Streitbeilegungsverfahren ein. Der EDSA hat nach der Leitlinie sodann darüber zu entscheiden, ob und inwieweit der Einspruch maßgeblich und begründet ist.
Kaum veröffentlicht, kam die Leitlinie auch schon zur Anwendung. Bei dem Kurznachrichtendienst Twitter war es zwischen dem 5. September 2017 und dem 11. Januar 2019 zu einer Datenpanne gekommen. Die irische Datenschutzaufsichtsbehörde hatte den Vorfall untersucht und den betroffenen Aufsichtsbehörden einen Beschlussentwurf vorgelegt, nach dem gegen die Twitter International Company wegen Verstößen gegen Art. 33 DS-GVO ein Bußgeld in Höhe von 135 000 bis 275 000 Euro zu verhängen sei. Mehrere europäische Aufsichtsbehörden legten gegen den Entscheidungsentwurf Einspruch ein, darunter Hamburg, Berlin, Baden-Württemberg, Niedersachsen und wir. Einer der Hauptkritikpunkte betraf die Höhe des vorgeschlagenen Bußgeldes. Die Verhängung einer Geldbuße hat nach Art. 83 Abs. 1 DS-GVO in jedem Einzelfall wirksam, verhältnismäßig und abschreckend zu sein. Eine Geldbuße in Höhe von 0,005 % bis 0,01 % des Jahresumsatzes ist nach Auffassung der deutschen Aufsichtsbehörden weder wirksam noch abschreckend. Die irische Aufsichtsbehörde ließ das Argument jedoch nicht gelten und leitete ein Streitbeilegungsverfahren vor dem EDSA ein. Dieser beauftragte die Enforcement Subgroup, die erste verbindliche Entscheidung des EDSA in einem Verfahren nach Art. 65 Abs. 1 DS-GVO vorzubereiten. Die Enforcement Subgroup kam in ihren Beratungen unter anderem zu dem Ergebnis, dass die Prinzipien der Wirksamkeit und Abschreckung bei der Berechnung des Bußgeldes nicht hinreichend berücksichtigt worden seien und die irische Aufsichtsbehörde daher dazu aufgefordert werden sollte, das Bußgeld neu zu berechnen.
Keine vertiefte Auseinandersetzung fand unter anderem zu der Frage statt, ob die Twitter International Company wirklich alleinverantwortlich agierte oder ob sie nicht vielmehr mit der Twitter Inc als gemeinsam Verantwortliche einzustufen war. Das lag daran, dass die Enforcement Subgroup keinen der Einsprüche, die diese Frage thematisierten, als „begründet“ einstufte. Der Subgroup fehlten Ausführungen zu den vom Beschlussentwurf in dieser Hinsicht ausgehenden Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen.

Dabei liegen diese bei Unklarheiten über die Verantwortlichen an sich auf der Hand. Die Leitlinien setzen die Schwelle für die Einlegung eines maßgeblichen und begründeten Einspruchs recht hoch, obwohl sich dies aus unserer Sicht nicht unbedingt der DS-GVO entnehmen lässt. Nach Art. 60 Abs. 4 DS-GVO ist ein Streitbeilegungsverfahren in jedem Fall einzuleiten, unabhängig davon, ob der Einspruch nach Ansicht der federführenden Aufsichtsbehörde maßgeblich und begründet ist oder nicht.

3.3 Technology Subgroup

Die Technology Subgroup ist eines von mehreren offiziellen Gremien (Expert-Group) des Europäischen Datenschutzausschusses (EDSA), siehe Punkt 3.1, in dem die Aktivitäten aller europäischen Datenschutzaufsichtsbehörden koordiniert werden. Die Bedeutung der Expert-Groups ist dabei enorm, denn eine europaweit einheitliche Auslegung der Europäischen Datenschutz-Grundverordnung (DS-GVO) kann nur durch einen regelmäßigen Meinungsaustausch und durch eine gemeinsame Meinungsbildung zwischen den europäischen Mitgliedsstaaten gewährleistet werden.
Wie der Arbeitskreis Technische und organisatorische Datenschutzfragen (AK Technik) auf nationaler Ebene, siehe Punkt 4.2, dient die Technology Subgroup im internationalen Kontext als ein Beratungs- und Unterstützungsgremium in Bezug auf Fragen zum technischen und organisatorischen Datenschutz. Um die Synergieeffekte der sich überschneidenden Themen in der Technology Subgroup und dem AK Technik sinnvoll zu nutzen, waren wir bis zum August des Berichtszeitraumes in diesem Gremium ein ständiger Vertreter der deutschen Landesdatenschutzbeauftragten. So war es uns einerseits möglich, den AK Technik über die laufenden Entwicklungen im europäischen Rahmen zu informieren, und andererseits erlaubte uns die Mitgliedschaft, wichtige nationale Themen und Standpunkte des AK Technik auf internationaler Ebene einzubringen bzw. zu vertreten.
Da sich mit dem Inkrafttreten der DS-GVO im Jahr 2018 die Bedeutung der Technology Subgroup deutlich erhöht hat, sind auch die Treffen von ehemals fünf Sitzungen im Jahr auf nunmehr elf Sitzungen angehoben worden. Da der Landtag und die Landesregierung nach wie vor dem gesteigerten Arbeitsaufwand nicht ausreichend Rechnung tragen, siehe auch Punkt 2, sahen wir uns nach über zehn Jahren gezwungen, diese wichtige Vertretung an die Berliner Beauftragte für Datenschutz und Informationsfreiheit abzugeben.
Im Berichtszeitraum lag ein Schwerpunkt der Arbeit der Technology Subgroup in der Erstellung von Papieren zur Einhaltung des Datenschutzes während der Corona-Pandemie. So wurde eine Leitlinie mit datenschutzrechtlichen Anforderungen bei der Nutzung von Standortdaten und Kontaktnachverfolgungen im Rahmen der europaweiten Contact Tracing Apps[1] (in Deutschland die Corona-Warn-App) erarbeitet. Aus deutscher Sicht war hier insbesondere die Einarbeitung des in Deutschland verwendeten dezentralen Modells von besonderer Bedeutung. Zudem wurden datenschutzrechtliche Anforderungen für den geplanten Datenaustausch der vorhandenen Contact Tracing Apps zwischen den Mitgliedsstaaten formuliert.

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

Neben den Diskussionen rund um das Thema Datenschutz bei der Pandemiebekämpfung, wurden auch eine Leitlinie mit Anforderungen an die Verarbeitung von personenbezogenen Daten im Kontext von vernetzten Fahrzeugen und Mobilitätsanwendungen[2] erstellt und diverse Anfragen von Mitgliedern des Europäischen Parlaments beantwortet.

3.4 Das europäische Binnenmarkt-Informationssystem (IMI)

In Mecklenburg-Vorpommern ist grundsätzlich der Landesbeauftragte für Datenschutz und Informationsfreiheit für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihm durch die Europäische Datenschutz-Grundverordnung (DS-GVO) übertragen wurden, zuständig. Bei grenzüberschreitenden Verarbeitungen ist jedoch die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen in der Europäischen Union (EU) federführend.
Das bedeutet, dass wir weiterhin für die Entgegennahme von Beschwerden über eine rechtswidrige Datenverarbeitung, beispielsweise durch Facebook, zuständig sind. Federführend bei der Entscheidung in der Sache sind jedoch in diesem Beispiel die Kollegen von der irischen Data Protection Commission. Sie legen einen Entscheidungsentwurf vor. Wenn wir als betroffene Aufsichtsbehörde mit dieser Entscheidung nicht einverstanden sind, können wir dagegen Einspruch einlegen. Schließt sich die irische Aufsichtsbehörde diesem Einspruch nicht an, haben sie das sogenannte Kohärenzverfahren einzuleiten, das in einem verbindlichen Beschluss des Europäischen Datenschutzausschusses (EDSA) mündet.
Jeder einzelne der für die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden erforderlichen Verfahrensschritte ist im Binnenmarkt-Informationssystem (IMI) abgebildet. Dabei handelt es sich um ein mehrsprachiges Online-Tool, das die Behörden bei der grenzüberschreitenden Verwaltungszusammenarbeit in mehreren Politikbereichen des Binnenmarkts, nicht nur im Bereich des Datenschutzes, unterstützt.
Seit dem 25. Mai 2018 fand in 2 083 Fällen über IMI eine Verständigung über die federführende Aufsichtsbehörde statt. 1 392 Fälle grenzüberschreitender Datenverarbeitungen fanden Eingang in das IMI-Fallregister. Davon gingen 1 001 Fälle auf eine Beschwerde zurück. Die übrigen Verfahren wurden von Amts wegen eingeleitet, etwa auf der Grundlage eigener Ermittlungen oder wegen eines Medienberichts. 512 Entscheidungsentwürfe haben die federführenden Aufsichtsbehörden über IMI an die betroffenen Aufsichtsbehörden weitergeleitet. Daraus sind bislang 168 endgültige Entscheidungen hervorgegangen. Wir haben bei insgesamt 16 Beschwerden über grenzüberschreitende Verarbeitungen ein IMI-Verfahren eingeleitet.

3.5 Erarbeitung von Leitlinien

Die Key Provisions Subgroup des Europäischen Datenschutzausschusses (EDSA) ist dabei, Leitlinien über das Recht auf Auskunft zu erarbeiten. Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat sie ein Recht auf Auskunft über diese Daten und auf die in Art. 15 Abs. 1 DS-GVO genannten Informationen. Da diese Informationen mitunter recht umfangreich sein können, wird mit Blick auf ihre Bereitstellung ein Mehrebenen-Ansatz diskutiert.

[2] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en

Danach soll die betroffene Person zunächst einen Überblick über sie betreffende Verarbeitungen erhalten, um auf diese Weise in die Lage versetzt zu werden, beim Verantwortlichen gezielt den Teil der Informationen zu erfragen, der für sie interessant ist. Wichtig ist uns dabei, dass ein solcher Mehrebenen-Ansatz den Verantwortlichen nicht von seiner Verpflichtung entbinden kann, die betroffene Person vollständig zu informieren.
Wenn die betroffene Person ihr Auskunftsrecht ausübt, hat ihr der Verantwortliche nach Art. 15 Abs. 3 Satz 1 DS-GVO eine Kopie der personenbezogenen Daten zur Verfügung stellen, die Gegenstand der Verarbeitung sind. So hat etwa ein Patient, der von seinem Arzt Auskunft nach Art. 15 Abs. 1 DS-GVO verlangt, das Recht auf Erhalt einer Kopie seiner Patientenakte. Nach Art. 15 Abs. 4 DS-GVO darf das Recht auf Erhalt einer Kopie nicht die Rechte und Freiheiten anderer Personen beeinträchtigen. Eine Kopie kann etwa personenbezogene Daten Dritter enthalten. Das darf aber nicht dazu führen, dass die betroffene Person überhaupt keine Kopie erhält, sondern höchstens dazu, dass die entsprechenden Passagen unkenntlich gemacht werden. Mehrere europäische Aufsichtsbehörden beziehen diese Einschränkung des Rechts auf Erhalt einer Kopie auf das Recht auf Auskunft insgesamt. Eine Auslegung des Art. 15 Abs. 4 DS-GVO contra legem, gegen den klaren Wortlaut der Norm, kommt jedoch für uns nicht in Betracht. Wir haben diese Sichtweise in die Beratungen zu der Leitlinie eingebracht, inwieweit sie Berücksichtigung finden wird, ist allerdings noch offen.
Ebenfalls begonnen hat die Key Provisions Subgroup mit den Arbeiten an den Leitlinien über die Verarbeitung personenbezogener Daten zur Wahrnehmung der berechtigten Interessen des Verantwortlichen oder eines Dritten. Diese ist nach Art. 6 Abs. 1 Buchstabe f DS-GVO zulässig, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Schon die Vorgängerin des EDSA, die Artikel-29-Datenschutzgruppe, hatte zu diesem Thema umfangreiche Leitlinien herausgegeben, die nun allerdings einer Überarbeitung bedürfen. Um festzustellen, in welchen Bereichen der Bedarf an Erläuterung und Konkretisierung besonders groß ist, organisierte der EDSA ein Stakeholder-Event, eine Art Verbandsanhörung, zu der über 60 Interessenvertreter aus der Wirtschaft, aber auch aus staatlichen sowie nichtstaatlichen Organisationen eingeladen wurden. Die Veranstaltung fand in Form einer Videokonferenz statt. Zusammen mit Baden-Württemberg übernahmen wir die Moderation eines der vier Workshops und befragten die Teilnehmer zu ihren praktischen Erfahrungen mit der Vorschrift.
Bei der Arbeit an den Leitlinien sollte aus unserer Sicht die Einschränkung der Profilbildung zu Werbezwecken im Vordergrund stehen. Wir werden deutlich machen, dass bei der nach Art. 6 Abs. 1 Buchstabe f DS-GVO erforderlichen Abwägung insbesondere der Umfang der verarbeiteten Daten eine Rolle spielt. In Fällen, in denen mehr oder weniger detaillierte Persönlichkeitsprofile der betroffenen Personen erstellt werden, überwiegen nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) in der Regel die Interessen der betroffenen Personen. Das muss aus unserer Sicht auch in den Leitlinien über die Verarbeitung personenbezogener Daten zur Wahrnehmung der berechtigten Interessen des Verantwortlichen oder eines Dritten berücksichtigt werden, für die bislang allerdings lediglich allererste Arbeitsentwürfe vorliegen.

3.6 Das Schrems-II-Urteil des EuGH

In seinem Urteil vom 16. Juli 2020 hat der Europäische Gerichtshof (EuGH) den Angemessenheitsbeschluss der Europäischen Kommission zum EU-US-Datenschutzschild für ungültig erklärt. Damit ist eine wesentliche Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA entfallen. Das Urteil betrifft eine Vielzahl von Betriebssystemen und Anwendungen, die sowohl in der Landesverwaltung als auch in der Privatwirtschaft genutzt werden.

Wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, darf ein Verantwortlicher nach Art. 46 Abs. 1 DS-GVO personenbezogene Daten an ein Drittland nur übermitteln, sofern er geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Diese geeigneten Garantien können nach Art. 46 Abs. 2 DS-GVO unter anderem in Standarddatenschutzklauseln bestehen, die von der Europäischen Kommission erlassen werden.
Der EuGH stellt in seinem Urteil klar, dass durch diese Garantien für Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein Schutzniveau gewährleistet sein muss, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist. Kein ausreichendes Mittel, um den effektiven Schutz der in das Drittland übermittelten personenbezogenen Daten zu gewährleisten, sind Standarddatenschutzklauseln in den Fällen, in denen „das Recht dieses Drittlands dessen Behörden Eingriffe in die Rechte der betroffenen Personen bezüglich dieser Daten erlaubt". Genau das ist aber in den USA der Fall.
Nach Section 702 des Foreign Intelligence Surveillance Act (FISA) können der Justizminister und der Direktor der nationalen Nachrichtendienste nach Billigung durch den Foreign Intelligence Surveillance Court (FISC) gemeinsam zur Beschaffung von „Informationen im Bereich der Auslandsaufklärung" die Überwachung von Personen genehmigen, die keine amerikanischen Staatsbürger (Nicht-US-Personen) sind und sich außerhalb des Hoheitsgebietes der Vereinigten Staaten aufhalten. Die Vorschrift dient als Grundlage für die Überwachungsprogramme PRISM und UPSTREAM. Im Rahmen des PRISM-Programms sind die Anbieter von Internetdiensten dazu verpflichtet, der National Security Agency (NSA) die gesamte Kommunikation vorzulegen, die von einer unter einen „Selektor" fallenden Person versandt oder empfangen worden ist. Ein Teil davon wird auch dem Federal Bureau of Investigation (FBI) und der Central Intelligence Agency (CIA) übermittelt. Im Rahmen des UPSTREAM-Programms sind die Telekommunikationsunternehmen, die das „backbone" (Rückgrat) des Internets - ein Netz von Kabeln, Switches und Routern - betreiben, verpflichtet, der NSA zu gestatten, die Internetverkehrsflüsse zu kopieren und zu filtern, um Zugang zu der Kommunikation zu erlangen, die von einer unter einen „Selektor" fallenden Nicht-US-Person versandt oder von ihr empfangen worden ist oder sie betrifft. Im Rahmen dieses Programms hat die NSA Zugriff sowohl auf die Metadaten als auch auf den Inhalt der betreffenden Kommunikation.
Die Executive Order (E.O.) 12333 erlaubt der NSA den Zugang zu Daten, die „auf dem Weg" in die Vereinigten Staaten sind, mittels Zugriff auf die am Grund des Atlantiks verlegten Seekabel, sowie die Sammlung und Speicherung dieser Daten, bevor sie in den Vereinigten Staaten ankommen und dort den Bestimmungen des FISA unterliegen. Die auf die E.O. 12333 gestützten Tätigkeiten sind nicht gesetzlich geregelt.
Zu den auf Section 702 des FISA und auf die E.O. 12333 gestützten Überwachungsprogrammen stellt der EuGH in seinem Urteil fest, dass weder die Presidential Directive 28 noch die E.O. 12333 den betroffenen Personen Rechte verleihen, die sie gegenüber den amerikanischen Behörden gerichtlich durchsetzen könnten. Den betroffenen Personen stehen somit keine wirksamen Rechtsbehelfe zur Verfügung.
Reichen Standarddatenschutzklauseln nicht aus, um einen effektiven Schutz der in das Drittland übermittelten personenbezogenen Daten zu gewährleisten, sind zusätzliche Maßnahmen, wie eine Verschlüsselung der Daten, in Erwägung zu ziehen. Nun sind jedoch unter Section 702 des FISA fallende Datenimporteure dazu verpflichtet, Zugang zu den von ihnen importierten personenbezogenen Daten zu gewähren oder diese herauszugeben. Das kann sich auch auf die kryptographischen Schlüssel erstrecken, die notwendig sind, um die Daten lesbar zu machen.

Wenn aber das Recht des Drittlandes dem Empfänger von aus der Union übermittelten personenbezogenen Daten Verpflichtungen auferlegt, die dazu geeignet sind, die vertragliche Garantie eines angemessenen Schutzniveaus zu untergraben, ist die Übermittlung nach dem Urteil des EuGH auszusetzen oder zu beenden. Konkret bedeutet dies, dass Betriebssysteme, Büro-Anwendungen oder auch Videokonferenzlösungen, die sich nicht betreiben lassen, ohne dass personenbezogene Daten an Server mit Standort in den USA übermittelt werden, ersetzt werden müssen.

3.7 Beschwerden gegen Datenübermittlungen in die USA

Einen Monat, nachdem der Europäische Gerichtshof (EuGH) den Angemessenheitsbeschluss der Europäischen Kommission zum EU-US-Datenschutzschild für ungültig erklärt hatte, analysierte das Europäische Zentrum für digitale Rechte („My Privacy is None of your Business - noyb“) die Quellcodes einer Vielzahl von europäischen Internetseiten und stellte fest, dass diese noch immer Google Analytics oder Facebook Connect benutzen. Die Nichtregierungsorganisation startete ein Projekt, in dessen Folge bei einer Reihe von europäischen Aufsichtsbehörden Beschwerden gegen 101 Unternehmen in 30 EU- und EWR-Mitgliedstaaten eingereicht wurden, die sich dieser Dienste nach wie vor bedienen. In Deutschland betrifft dies unter anderem die FUNKE Digital GmbH und die TV Spielfilm Verlag GmbH.
Mit Blick auf den Dienst Facebook Connect tragen die Beschwerdeführer vor, die Webseite des jeweiligen Beschwerdegegners besucht zu haben, während sie in ihr Facebookbenutzerkonto eingeloggt waren. Auf der Website habe der Beschwerdegegner den HTML-Code für Facebook-Dienste (einschließlich Facebook Connect) eingebettet. Facebook Connect sei ein von Webseiten Dritter genutzter Dienst, der die Übertragung personenbezogener Daten des Benutzers zwischen der Website und Facebook auslöse. Die Nutzung von Facebook Connect unterliege den Nutzungsbedingungen für Facebook Business-Tools und den Facebook-Datenverarbeitungsbedingungen. Beide Dokumente seien mit Wirkung zum 31. August 2020 aktualisiert worden. Danach sei Facebook Ireland als Auftragsverarbeiter des Beschwerdegegners und die Facebook Inc als Sub-Auftragsverarbeiter zu qualifizieren.
Im Verlauf des Webseitenbesuchs habe der Beschwerdegegner die Beschwerdeführer betreffende personenbezogene Daten verarbeitet, zumindest die IP-Adresse und Cookie-Daten. Zumindest einige dieser Daten habe der Beschwerdegegner an die Facebook Inc in den USA übermittelt. Eine solche Übermittlung erfordere eine Rechtsgrundlage nach den Art. 45 ff. DS-GVO. Den Angemessenheitsbeschluss der Europäischen Kommission zum EU-US-Datenschutzschild habe der EuGH für ungültig erklärt. Dennoch würden sich die Facebook-Gruppe und der Beschwerdegegner weiterhin auf das EU-US-Datenschutzschild stützen. Ein System zur regelmäßigen Datenübermittlung, das auf einer für ungültig erklärten Angemessenheitsentscheidung basiere, stellt aus Sicht der Beschwerdeführer eine schwerwiegende, systematische und im Hinblick auf die Neuen Facebook-Datenverarbeitungsbedingungen zudem vorsätzliche Verletzung der Art. 45 ff. DS-GVO dar. Die Beschwerden über den Dienst Google Analyics lesen sich ähnlich.
Inzwischen stützen sich Facebook und Google auf die sogenannten Standardvertragsklauseln der Europäischen Union. Ob sie dafür die vom EuGH geforderten „zusätzlichen Maßnahmen“ als Ergänzung der Standardvertragsklauseln ergriffen haben und ob diese Maßnahmen ausreichen, um das vom EuGH geforderte Schutzniveau in den USA zu gewährleisten, ist aus Sicht der deutschen Aufsichtsbehörden zur inhaltlichen Kernfrage der Beschwerdeverfahren geworden.

Wegen des grenzüberschreitenden Charakters der darin monierten Datenverarbeitungen unterliegen die Beschwerden dem Verfahren der Zusammenarbeit nach den Artikeln 60 ff. DS-GVO. Der Europäische Datenschutzausschuss (EDSA) hat eine Task Force ins Leben gerufen, um eine schnelle und europaweit einheitliche Bearbeitung der Beschwerden zu gewährleisten.

4 Zusammenarbeit auf deutscher Ebene

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

In diesem Berichtszeitraum tagte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) unter dem Vorsitz des Sächsischen Datenschutzbeauftragten.
Von den zwei regulären Konferenzen und den drei zusätzlichen Zwischenkonferenzen konnte nur die 1. Zwischenkonferenz unter den gewohnten Sitzungsbedingungen als Präsenzveranstaltung durchgeführt werden. Die Einschränkungen der Corona-Pandemie führten dazu, dass alle anderen Datenschutzkonferenzen als Videokonferenz stattfanden. Mit dem Videokonferenzsystem des Bundes, das über das besonders gesicherte Netz des Bundes betrieben wird, konnten wir dabei auf ein datenschutzkonformes, sicheres und komfortables Konferenzsystem zurückgreifen.
Die 99. Datenschutzkonferenz fand im Mai 2020 statt. Trotz des für alle Teilnehmenden neuen Formats als Videokonferenz konnte eine umfangreiche Tagesordnung abgearbeitet werden. Breiten Raum nahm der Bericht der deutschen Vertreter im Europäischen Datenschutzausschuss (EDSA) ein, siehe dazu auch Punkt 3.1. Unter anderem war festzustellen, dass auch auf europäischer Ebene Datenschutzfragen der Corona-Pandemie einen hohen Koordinierungsaufwand erfordern. Ein weiterer Schwerpunkt betraf Themen, die der von uns geleitete Arbeitskreis Technik, siehe Punkt 4.2, eingebracht hatte. So verabschiedete die Datenschutzkonferenz die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“[3] und eine umfassend überarbeitete Version des Standard-Datenschutz-Modells[4], siehe Punkt 7.1. Fortgesetzt wurden die Beratungen über Datenschutzaspekte von Produkten des amerikanischen Softwarekonzerns Microsoft wie Office 365 und Windows 10, siehe Punkte 7.2 und 7.3 und 15. Tätigkeitsbericht Punkte 7.1.2 und 7.1.4. Aber auch Fragen der Zusammenarbeit der Datenschutzaufsichtsbehörden innerhalb Deutschlands und auf internationaler Ebene wurden besprochen.
Angesichts der Vielzahl der aktuellen datenschutzrelevanten Themen in Wirtschaft und Verwaltung ist es zur Normalität geworden, dass die Datenschutzaufsichtsbehörden sich jedes Jahr zusätzlich zu den turnusmäßigen Sitzungen zu mehreren Zwischenkonferenzen treffen.
In der 1. Zwischenkonferenz im Januar 2020 erörterten die Teilnehmenden unter anderem das Thema „Digitale Souveränität“ und verabschiedeten ein Statement, das einen Beschluss des IT-Planungsrates zu diesem Thema[5] vorbereitete, siehe Punkt 4.3.4.

[3] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20200512_OH_E-Mail-Verschl%C3%BCsselung.pdf
[4] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf
[5] https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2020/Sitzung_31.html?nn=6848410&pos=6

In der 2. Zwischenkonferenz im Juni 2020 wurde das Thema Corona erneut aufgegriffen. In einer Pressemitteilung[6] lobte die Datenschutzkonferenz das datenschutzfreundliche Grundkonzept der Corona-Warn-App, warnte aber vor dem Untergraben der Freiwilligkeit durch zweckwidrige Nutzung der mit der App erhobenen Daten. Die Datenschutzkonferenz beauftragte zudem ihren Arbeitskreis Verwaltung, ein Konzept zu erarbeiten, wie die Datenschutzaufsichtsbehörden die Umsetzung des Onlinezugangsgesetzes (OZG) in ihren jeweiligen Zuständigkeitsbereichen begleiten können und wie die Zusammenarbeit mit dem IT-Planungsrat auf diesem Gebiet weiter ausgebaut werden kann, siehe auch Punkt 4.3.3.
Die 3. Zwischenkonferenz im September 2020 setzte eine Arbeitsgruppe ein, die sich mit den Auswirkungen des EuGH-Urteils „Schrems II“ befassen soll, siehe dazu auch Punkt 3.6. Als Reaktion auf das Urteil des EuGH vom 9. Juli 2020 zur Geltung der Europäischen Datenschutz-Grundverordnung (DS-GVO) in Parlamenten wurde ein Beschluss der Datenschutzkonferenz aus dem Jahr 2018[7] zunächst ausgesetzt. In dieser Zwischenkonferenz wurde aber auch eine Reihe von Themen aus vorangegangenen Datenschutzkonferenzen erneut aufgegriffen. So verabschiedete die Datenschutzkonferenz eine Entschließung zum Thema „Digitale Souveränität“[8] und veröffentlichte als Anlage zum Protokoll der Konferenz[9] eine datenschutzrechtliche Bewertung von Microsoft Office 365, siehe auch Punkt 7.2. Schließlich wurde auch eine überarbeitete Version des Kurzpapiers Nr. 14 „Beschäftigtendatenschutz“ der Datenschutzkonferenz verabschiedet[10].
Die 100. Datenschutzkonferenz im November 2020 sollte ursprünglich in einem besonders festlichen Rahmen in Dresden stattfinden. Aber auch diese mit viel Aufwand und Engagement vorbereitete Jubiläumskonferenz fiel der Corona-Pandemie zum Opfer und musste als Videokonferenz stattfinden. Erneut befasste sich die Datenschutzkonferenz mit Office 365 und den von Microsoft angekündigten Verbesserungen des Datenschutzes, siehe Punkt 7.2. In einem Beschluss[11] erläuterte die Datenschutzkonferenz ihre Untersuchungsergebnisse zu den Telemetriefunktionen von Microsoft Windows 10 und sprach Empfehlungen für die Anwender dieses Betriebssystems aus, siehe Punkt 7.3.
Wenige Tage vor der 100. Datenschutzkonferenz waren die Forderungen der Regierungen der Mitgliedstaaten der Europäischen Union bekannt geworden, Sicherheitsbehörden und Geheimdiensten die Möglichkeit zu eröffnen, auf Inhalte verschlüsselter Kommunikation zuzugreifen. In ihrer Entschließung[12] weist die Datenschutzkonferenz darauf hin, dass die Aushöhlung von Verschlüsselungslösungen, wie sie vom Rat der Europäischen Union nahegelegt wird, kontraproduktiv wäre und durch Kriminelle und Terroristen leicht umgangen werden könnte. Klar lehnt die Datenschutzkonferenz Forderungen nach einem Zugriff der Sicherheitsbehörden und Geheimdienste auf die verschlüsselte Kommunikation in Messengerdiensten und der privaten Kommunikation ab.

6 https://www.datenschutz-mv.de/presse/?id=161116&processor=processor.sa.pressemitteilung
7 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/bes_Anw_Parl.pdf
8 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20200922_Ent_digitale_-Souveraenitaet.pdf
9 https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf
10 https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_14.pdf
11 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20201126_Beschluss_Telemetrie_Win10_Enterprise.pdf
12 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20201125_%20Ent_-chutz_vertrauliche_Kommunikation.pdf

Mit einer weiteren Entschließung[13] appelliert die Datenschutzkonferenz an den Bundesgesetzgeber, endlich die Vorgaben des Bundesverfassungsgerichts vom Mai 2020 zur Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens umzusetzen. Die Datenschutzkonferenz fordert die Gesetzgeber in Bund und Ländern auf, das manuelle Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste möglichst rasch verfassungskonform auszugestalten.
Des Weiteren fordert die Datenschutzkonferenz den Gesetzgeber auf, endlich die ePrivacy-Richtlinie der Europäischen Gemeinschaften aus dem Jahr 2002 (RL 2002/58/EG) vollständig und im Einklang mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) von 2018 in deutsches Recht umzusetzen. In ihrer Entschließung[14] betont die Datenschutzkonferenz ihre Auffassung, dass das Urteil des Bundesgerichtshofs (BGH) vom 28. Mai 2020 (I ZR 7/16 - „Planet49“) den seit langem bestehenden dringenden Handlungsbedarf verstärkt.
Deutlich wendet sich die Datenschutzkonferenz auch gegen Forderungen nach einer Zentralisierung der Datenschutzaufsicht im nicht-öffentlichen Bereich. Der Vorsitzende der Datenschutzkonferenz erklärte dazu: „Die Aufsichtsbehörden in Bund und Ländern genießen fachlich hohes Ansehen. Ihre Zentralisierung wäre ausgesprochen kontraproduktiv, denn Zentralisierung heißt auch, immer weiter weg von den Anliegen und konkreten Umständen der betroffenen Menschen zu sein. Statt unnötiger Zentralisierungsdebatten sollte dafür gesorgt werden, dass alle Aufsichtsbehörden personell und organisatorisch ihre gesetzlichen Aufgaben vollauf erfüllen können.“

4.2 AK Technik

Die Datenschutzkonferenz (DSK) hat zu ihrer fachlichen Unterstützung Arbeitskreise zu verschiedenen Themen gegründet. Über den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) haben wir regelmäßig berichtet, zuletzt im Fünfzehnten Tätigkeitsbericht unter Punkt 5.2. Die Datenschutzkonferenz hat uns die Leitung dieses Arbeitskreises seit vielen Jahren anvertraut.
Zum Schutz vor der Lungenkrankheit COVID-19 wurden seit Beginn des Jahres 2020 weltweit umfangreiche Infektionsschutzmaßnahmen getroffen, siehe auch Punkt 5. Diese haben auch die Tätigkeit des Arbeitskreises sowohl inhaltlich als auch organisatorisch beeinflusst. Dennoch tagte der Arbeitskreis auch im Berichtszeitraum wie gewohnt zweimal. An den Sitzungen nahmen auch wieder ständige Gäste aus dem deutschsprachigen Ausland und von den spezifischen Datenschutzaufsichtsbehörden der großen christlichen Kirchen und des Rundfunks teil.
Die 74. Sitzung konnte noch als anderthalbtägige Präsenzveranstaltung beim Bayerischen Landesbeauftragten für den Datenschutz in München stattfinden. Die Teilnehmerinnen und Teilnehmer konnten sich zu Beginn über ein Verfahren zur Auskunft von Telekommunikationsunternehmen an Strafverfolgungsbehörden informieren.

[13] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20201125_Ent_Auskunftsverfahren_verfassungskonform_ausgestalten.pdf

[14] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20201125_Ent_Rechtssicherheit_ePrivacy-Richtlinie.pdf

Es folgten Vorträge zur Datenschutzorganisation an der Technischen Universität München und zu Angeboten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an Bund, Länder und Kommunen. Wir führten die Diskussionen zu den Themen Windows 10 weiter und konnten die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ beschließen. Darüber hinaus wurden das Standard-Datenschutz-Modell (SDM) ergänzt und neue Bausteine zum SDM verabschiedet, im Einzelnen „Protokollieren“, „Löschen und Vernichten“ und „Dokumentation“, siehe Punkt 7.1.
Die Infektionsschutzauflagen haben uns veranlasst, die 75. Sitzung als eintägige Videokonferenz auszurichten. Aus technischen Gründen konnten wir diesmal den ständigen Gästen nur eingeschränkte Teilnahmemöglichkeiten bieten. Außerdem mussten wir auf eingeladene Vorträge verzichten.
Die Datenschutzaufsichtsbehörden sind nicht nur selbst Nutzer oder Betreiber von Videokonferenzsystemen, sondern werden auch mit vielfältigen Anfragen zur datenschutzgerechten Auswahl und Anwendung solcher Systeme konfrontiert. Deshalb entstand innerhalb weniger Wochen die Orientierungshilfe „Videokonferenzsysteme“, siehe Punkt 5.1, deren Entwurf auf der Sitzung verabschiedet werden konnte. Es handelt sich dabei um ein Gemeinschaftswerk der Arbeitskreise Grundsatzfragen und Technik der DSK.
Darüber hinaus haben wir auf der Sitzung die Arbeiten zu Windows 10 abschließen können, sodass auf der 100. Datenschutzkonferenz zu diesem wichtigen Thema ein Beschluss gefasst werden konnte, siehe Punkt 7.3. Auch das Standard-Datenschutz-Modell stand wieder auf der Tagesordnung. Nach intensiver Vorarbeit der entsprechenden Unterarbeitsgruppe konnten wir die Bausteine „Berichtigen“, „Aufbewahren“, „Einschränken“ und „Trennen“ verabschieden, siehe Punkt 7.1.

4.3 IT-Planungsrat

Der Bericht über unsere Rolle als Vertreter der Landesdatenschutzbeauftragten in diesem wichtigen Gremium ist seit vielen Jahren fester Bestandteil unseres Tätigkeitsberichtes. Unsere aktive Mitwirkung im IT-Planungsrat hat an Bedeutung weiter zugenommen, weil die thematischen Überschneidungen in der Arbeit der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) und des IT-Planungsrates größer geworden sind. Der Abstimmungsbedarf zwischen den beiden Gremien hat daher zugenommen. Die Zusammenarbeit wurde auf der Ebene verschiedener Arbeitsgremien von Datenschutzkonferenz und IT-Planungsrat stetig ausgebaut. Während wir regelmäßig an den Sitzungen des IT-Planungsrates teilnehmen, sind zahlreiche Kolleginnen und Kollegen anderer Datenschutzaufsichtsbehörden in verschiedenen Arbeitsgremien des IT-Planungsrates aktiv und begleiten dessen Steuerungs- und Koordinierungsprojekte.

4.3.1 Turnusmäßige Sitzungen

Auch in diesem Berichtszeitraum haben wir sowohl an den drei turnusmäßigen Sitzungen als auch an den jeweiligen vorbereitenden Sitzungen auf der Ebene der Abteilungsleiter (AL) der für IT-Fragen zuständigen Landesressorts teilgenommen. Während die AL-Vorbesprechungen schon seit vielen Jahren als Videokonferenzen stattfinden, war es für den IT-Planungsrat neu, dass auch dessen Sitzungen als Reaktion auf die Corona-Pandemie als Videokonferenz stattfinden mussten. Dennoch konnten die Tagesordnungen der Sitzungen fast uneingeschränkt abgearbeitet werden. Aus datenschutzrechtlicher Sicht waren die im Folgenden ausführlicher erläuterten Themen Registermodernisierung, Umsetzung des Onlinezugangsgesetzes (OZG) und Digitale Souveränität von besonderer Bedeutung.

4.3.2 Registermodernisierung

Die Regierungschefinnen und Regierungschefs der Länder hatten bereits im Oktober 2018 den Beschluss gefasst, die Registermodernisierung unter Beteiligung der Länder umgehend zu starten, siehe 15. Tätigkeitsbericht Punkt 5.3.2. Im Berichtszeitraum sollte nun die aus datenschutzrechtlicher Sicht besonders wichtige Frage geklärt werden, welches Architekturmodell des Zugriffs auf die in staatlichen Registern gespeicherten personenbezogenen Daten umgesetzt werden soll: Der Architekturansatz „Einheitlicher Identifier“ oder der Architekturansatz „Bereichsspezifischer Identifier“. In zahlreichen Sitzungen verschiedener Arbeitsgremien des IT-Planungsrates haben wir gemeinsam mit unseren Kolleginnen und Kollegen anderer Datenschutzaufsichtsbehörden auf die Risiken von einheitlichen Identifiern hingewiesen und verschiedene grundrechtskonforme Lösungen für bereichsspezifische Identifier vorgeschlagen, etwa das österreichische Modell des Stammzahlensystems. Wir hatten jedoch nie den Eindruck, dass angesichts des hohen Zeitdrucks wirklich ernsthaft eine andere Architektur als die des zentralen Identifiers in Betracht gezogen wurde. Somit drohte die Schaffung einer bundesweiten einheitlichen Personenkennziffer.
So überraschte es dann auch wenig, als im Juli 2020 ein Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat bekannt wurde, der genau diese einheitliche Personenkennziffer beinhaltete. Der Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG) legt fest, dass als zentraler Identifier die sogenannte Steuer-ID verwendet werden soll. Dabei handelt es sich um die Identifikationsnummer nach § 139b der Abgabenordnung (AO), die als zusätzliches Ordnungsmerkmal in mehr als 50 Register des Bundes und der Länder eingeführt werden soll. Zudem wird das Bundesverwaltungsamt als Registermodernisierungsbehörde bestimmt. Das Amt soll ein neues Register aufbauen und führen, das neben der Steuer-ID weitere zur Identifizierung einer natürlichen Person erforderliche personenbezogene Daten (die sogenannten Basisdaten) enthält. Um unzulässige Datenübermittlungen zwischen öffentlichen Stellen zu verhindern, soll die Registermodernisierungsbehörde eine automatisierte Prüfung der übermittelten Daten daraufhin durchführen, ob sie der richtigen Identifikationsnummer zugeordnet, vollständig und schlüssig sind. Mit dieser Regelung wird jedoch nur ein Bruchteil aller Datenübermittlungen geprüft. Die an Datenübermittlungen beteiligten Stellen sollen nämlich sechs Bereichen zugeordnet werden: Inneres, Justiz, Wirtschaft und Finanzen, Arbeit und Soziales, Gesundheit, Statistik. Automatisiert geprüft werden nur bereichsübergreifende Übermittlungen.

Als massives datenschutzrechtliches Defizit ist deshalb die Tatsache zu bewerten, dass alle Übermittlungen, die innerhalb der sechs zu bildenden Bereiche stattfinden, ungeprüft bleiben.
In ihrer Entschließung vom 26. August 2020[15] hat die Datenschutzkonferenz erneut darauf hingewiesen, dass das Bundesverfassungsgericht (BVerfG) der Einführung derartiger Personenkennzeichen seit jeher enge Schranken auferlegt hat und dass der Gesetzentwurf diese Schranken missachtet. Der Blick auf den Anwendungsumfang der geplanten Regelung zeige das Potenzial der möglichen missbräuchlichen Verwendung. Künftig kann nicht sicher ausgeschlossen werden, dass Daten etwa aus dem Melderegister mit Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt oder dem Schuldnerverzeichnis abgeglichen und zu einem Persönlichkeitsprofil zusammengefasst werden. Die Datenschutzkonferenz weist nachdrücklich darauf hin, dass die dem Gesetzentwurf zugrundeliegende Architektur im Widerspruch zu verfassungsrechtlichen Regelungen steht. Sie hat deshalb die Bundesregierung aufgefordert, einen Entwurf vorzulegen, der den verfassungsrechtlichen Anforderungen genügt, bevor sie durch Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird.
Kritik kommt auch aus dem Deutschen Bundestag. In seinem Gutachten „Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes“[16] verweisen die Wissenschaftlichen Dienste des Deutschen Bundestages auf das Urteil des Finanzgerichtes Köln vom 7. Juli 2010. In seinen Ausführungen zur Verfassungsmäßigkeit der Einführung der Steuer-ID spräche das Gericht von einem strikten Verbot eines einheitlichen, für alle Register und Daten geltenden Personenkennzeichens. Das Gutachten bewertet die Steuer-ID in ihrer neuen Ausprägung wegen des Umfangs, der Verschiedenheit und der Tragweite der erfassten Verwaltungs- und Lebensbereiche aber als genau solch ein zentrales Personenkennzeichen für die gesamte Verwaltung von Bund und Ländern und künftig sogar für die Privatwirtschaft. Besonders problematisch sei die Tatsache, dass der Gesetzentwurf keine ausdrückliche Regelung enthält, dass die Nutzung der Identifikationsnummer zur Bildung von Persönlichkeitsprofilen unzulässig ist. Zudem sei die Zweckbindung der Verarbeitung der Identifikationsnummer nicht ausschließlich auf die Identifikation von Personen gegenüber der Verwaltung beschränkt. Somit sei die Nutzung der Steuer-ID in der Privatwirtschaft nicht ausgeschlossen. Das Gutachten kommt zum Ergebnis, dass die Abwägung der Gemeinwohlziele mit der Intensität des Eingriffs in die Grundrechte mindestens als offen anzusehen sei.
Im August 2020 haben wir die Ministerpräsidentin des Landes Mecklenburg-Vorpommern und den Minister für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern über unsere Kritik am Gesetzentwurf informiert und aufgefordert, im Bundesrat für einen vorläufigen Stopp des Gesetzentwurfs zu votieren und die Bundesregierung aufzufordern, einen Entwurf vorzulegen, der den verfassungsrechtlichen Anforderungen genügt, bevor sie durch Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird. Eine Reaktion auf diese Schreiben ist bis zum Redaktionsschluss dieses Berichts ausgeblieben.

Wir wiederholen unsere Empfehlung aus dem 15. Tätigkeitsbericht an die Landesregierung, sich dafür einzusetzen, dass bei der Modernisierung der Verwaltungsregister der verfassungskonforme Architekturansatz bereichsspezifischer Identifier beispielsweise in Anlehnung an das österreichische Stammzahlensystem umgesetzt wird und keine einheitlichen und verwaltungsübergreifenden Personenkennzeichen gebildet werden. Wir fordern die Landesregierung auf, im Bundesrat dem Entwurf des Registermodernisierungsgesetzes nicht zuzustimmen.

[15] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20200826_Ent_PKZ.pdf
[16] https://www.bundestag.de/resource/blob/793658/c8c9c4a28cf88a2ae31f81887ec293d9/WD-3-196-20-pdf-data.pdf

4.3.3 Umsetzung des Onlinezugangsgesetzes (OZG)

„Bund und Länder sind verpflichtet, bis spätestens zum Ablauf des fünften auf die Verkündung dieses Gesetzes folgenden Kalenderjahres ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten.“ Hinter diesem einleitenden Satz des Onlinezugangsgesetzes (OZG) versteckt sich eine gigantische Aufgabe für fast alle Bereiche der deutschen Verwaltung. Bis zum Ende des Jahres 2022 müssen 575 Angebote für Bürgerinnen, Bürger und Wirtschaft - von Anträgen auf Wohngeld bis zur Anmeldung eines Unternehmens - digital bereitgestellt werden.
Durch die Schaffung eines themenfeldübergreifenden Programmmanagements koordinieren die Föderale IT-Kooperation (FITKO) und das Bundesministerium des Innern, für Bau und Heimat (BMI) gemeinsam das Digitalisierungsprogramm. Richtungsweisende Entscheidungen für das Digitalisierungsprogramm werden durch den IT-Planungsrat getroffen und über das Programmmanagement umgesetzt. Um die flächendeckende Digitalisierung der Verwaltung Deutschlands bis 2022 realisieren zu können, hat der IT-Planungsrat das Einer-für-Alle-Prinzip ausgegeben. Jedes Land soll demnach Leistungen so digitalisieren, dass andere Länder sie nachnutzen können und den Online-Prozess nicht noch einmal selbst entwickeln müssen. Dieses Modell hat im Zuge des Corona-Konjunkturpakets nochmals an Relevanz gewonnen, da die Vergabe von Mitteln aus dem Konjunkturpaket an die Umsetzung des Einer-für-Alle-Prinzips geknüpft ist.
Die Federführung für die Digitalisierung von Leistungen im Themenfeld Bauen und Wohnen hat Mecklenburg-Vorpommern übernommen.
Auch die datenschutzrechtlichen Herausforderungen des Einer-für-Alle-Prinzips sind groß. Bei der Digitalisierung einer Verwaltungsdienstleistung müssen nämlich die datenschutzrechtlichen Rahmenbedingungen des künftigen Einsatzes in allen Bundesländern berücksichtigt werden. Die Datenschutzkonferenz hat dem IT-Planungsrat die Unterstützung angeboten. Sie hat ihren Arbeitskreis Verwaltung beauftragt, ein Arbeitspapier zu erstellen, welches die Anforderungen an eine datenschutzrechtliche Dokumentation für eine vereinfachte Nachnutzbarkeit der Anwendungen aus dem OZG-Leistungskatalog darstellt. Der Arbeitskreis hat zudem eine Arbeitsgruppe zur datenschutzrechtlichen Bewertung der OZG-Umsetzung von Portalen und auch Fachanwendungen eingerichtet, die die möglichen Konstellationen von Betreibermodellen in Bezug auf deren datenschutzrechtliche Verantwortlichkeit und Umsetzung prüft. Dem Bundesinnenministerium und dem IT-Planungsrat wurde ein stetiger Austausch angeboten. In seiner 33. Sitzung im Oktober 2020 haben wir den IT-Planungsrat über dieses Angebot informiert.

Wir empfehlen der Landesregierung, bei der Digitalisierung von Verwaltungsdienstleistungen im Rahmen des Einer-für-alle-Prinzips frühzeitig die datenschutzrechtlichen Rahmenbedingungen zu berücksichtigen, das Beratungsangebot der Datenschutzkonferenz in Anspruch zu nehmen und uns frühzeitig in die Entwicklung der digitalen Angebote einzubeziehen.

4.3.4 Digitale Souveränität

Die Datenschutzkonferenz warnt schon seit vielen Jahren vor Intransparenz von Informationstechnik und vor der Abhängigkeit von Wirtschaft und Verwaltung von monopolartig organisierten Anbietern von Hard- und Software. Bereits im Jahr 1999 hat die Datenschutzkonferenz in ihrer Entschließung „Transparente Hard- und Software“[17] Hersteller aufgefordert, Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.
Wie aktuell das Thema auch heute ist, zeigt eine vom Bundesministerium des Innern, für Bau und Heimat (BMI) beauftragte strategische Marktanalyse[18]. Diese untermauert die zunehmend kritische Technologieabhängigkeit der Öffentlichen Verwaltung in Deutschland, aber auch im europäischen Umfeld. Die Analyse offenbart auch Risiken insbesondere im Kontext der Telemetriedaten-Übermittlung von Software-Produkten sowie der international heterogenen Rechtsetzung, siehe dazu beispielsweise Punkt 7.3.
In seinem Eckpunktepapier[19] zur Digitalen Souveränität vom 31. März 2020 fordert der IT-Planungsrat folgerichtig Interoperabilität sowie offene Standards und Schnittstellen. Alternativen sollten vorzugsweise, aber nicht zwingend, auf quelloffenen und freien Software-Produkten basieren, mindestens jedoch auf offenen Standards und Schnittstellen. Hier decken sich die Auffassungen des IT-Planungsrates und der Datenschutzkonferenz sehr weitgehend. In ihrer Entschließung vom September 2020[20] fordert die Konferenz erneut, nur solche Hard- und Software einzusetzen, die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt. Alle zur Verfügung stehenden Sicherheitsfunktionen müssen für Verantwortliche transparent sein. Die Nutzung der Hard- und Software sowie der Zugriff auf personenbezogene Daten müssen möglich sein, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können. Die Datenschutzkonferenz ist der Ansicht, dass die Stärkung der Digitalen Souveränität große strategische Bedeutung für die öffentliche Verwaltung hat und gemeinsam und kontinuierlich vorangetrieben werden muss.
Diese Forderungen gelten uneingeschränkt für Wirtschaft und Verwaltung des Landes Mecklenburg-Vorpommern. Zurzeit können wir jedoch keine Strategie der Landesregierung erkennen, die zumindest in der Landesverwaltung zu der oben beschriebenen Digitalen Souveränität führt. Nach wie vor werden in großem Umfang Hard- und Softwareprodukte eingesetzt, die zu einer hochriskanten Abhängigkeit von einzelnen Herstellern führen. Selbst bei der Neukonzeption von Verfahren spielen die von der Datenschutzkonferenz und vom IT-Planungsrat geforderten quelloffenen und freien Software-Produkte nur selten eine Rolle.

[17] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/ent57_hardsoftware.pdf
[18] https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.-pdf?__blob=publicationFile
[19] https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/32_Umlaufverfahren_Eckpunktepapier/Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf?__blob=publicationFile&v=3
[20] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20200922_Ent_digitale_Souveraenitaet.pdf

Wir empfehlen der Landesregierung, sowohl bei der Umsetzung des Onlinezugangsgesetzes (OZG) als auch bei der Weiterentwicklung der gesamten IT-Infrastruktur des Landes die Prinzipien der Digitalen Souveränität zu berücksichtigen. Dies erfordert eine umfassende, moderne IT-Strategie, die zu einer weitgehenden Unabhängigkeit von einzelnen Herstellern führen muss. Von der Entwicklung des Standardarbeitsplatzes im Rahmen des Projektes „MV-PC“ über die Erarbeitung neuer Strukturen für die E-Akte bis hin zu strategischen Überlegungen hinsichtlich der gesamten IT-Infrastruktur des Landes muss das Thema „Open Source“ eine zentrale Rolle spielen.

5 Corona

5.1 Videokonferenzsysteme

Videokonferenzsysteme erlangten mit Beginn der Corona-Pandemie große Aufmerksamkeit. Das Thema ist nicht neu, fristete bisher jedoch eher ein Nischendasein. Als Folge der Pandemie hat die Kommunikation über Videokonferenzsysteme in kürzester Zeit jedoch in nahezu allen Lebensbereichen ihren Einzug gehalten. Die Vorteile liegen dabei auf der Hand. Das Arbeiten aus dem Homeoffice wird erleichtert und die Zahl der Dienstreisen drastisch minimiert. Die Kommunikation erfolgt bei Bedarf mit Sichtkontakt und zudem können gleichzeitig Dokumente präsentiert werden, an denen während der Konferenz gemeinsam gearbeitet werden kann.
Diese für viele recht neue Art der Kommunikation führte jedoch auch zu vielen Unsicherheiten, sowohl bei den Teilnehmenden als auch den für die Videokonferenz Verantwortlichen. Das führte folgerichtig zu einer großen Anzahl von Beschwerden und Beratungsgesprächen. Wir erhielten dabei Eingaben aus den unterschiedlichsten Bereichen, beispielsweise von Schulen oder Hochschulen, in denen der Lehrbetrieb auf einmal digital stattfinden musste. Aber auch in Wirtschaft und Verwaltung haben diese Systeme umfassenden Einzug gehalten und zu vielen Fragen geführt.
Zu Beginn der Pandemie wurden oftmals kostengünstige und schnell verfügbare Videokonferenzsysteme eingesetzt, oft jedoch ohne die dabei notwendigen datenschutzrechtlichen und technischen Rahmenbedingungen zu beachten. Nicht immer wurde berücksichtigt, dass im Rahmen von Videokonferenzen eine Vielzahl von personenbezogenen Daten der teilnehmenden Personen verarbeitet wird, mitunter auch höchst sensible. Betroffen sind einerseits die inhaltlichen Äußerungen und die Übertragung von Ton und Bild der teilnehmenden Personen und gegebenenfalls ihres Umfeldes (Inhaltsdaten), andererseits aber auch die Metadaten über die Durchführung der Kommunikation (Rahmendaten). Hinzu kommen Daten über die beruflichen Kontakte, die Anwesenheits- und Arbeitszeiten und gegebenenfalls daraus ableitbar auch Daten über die Arbeitsleistung. Neben den Inhalts- und Rahmendaten können aber auch noch andere personenbezogene Daten anfallen, beispielsweise die videokonferenzbegleitenden Chatnachrichten, Daten aus in der Konferenz präsentierten oder übermittelten Dokumenten und Daten von nicht teilnehmenden Personen, die im lokalen Umfeld eines Teilnehmers durch Bild oder Ton unbeabsichtigt mit aufgezeichnet werden.
Da bei der Durchführung von Videokonferenzen personenbezogene Daten verarbeitet werden, benötigt der für die Datenverarbeitung Verantwortliche hierfür eine Rechtsgrundlage. Um eine Videokonferenz rechtlich und technisch bewerten zu können, ist zunächst zu klären, welches Betriebsmodell zu Grunde liegt. Zu unterscheiden ist zwischen Videokonferenzsystemen, die entweder als Online-Dienst (Software as a Service), als ein selbst betriebenes System oder in Form eines Dienstes bei einem externen IT-Dienstleister betrieben werden.

Wegen der scheinbar einfachen Bereitstellung der Videokonferenz bei einem Online-Dienst werden die Anforderungen an rechtliche und technische Rahmenbedingungen, die den Schutz der personenbezogenen Daten gewährleisten sollen, oftmals unterschätzt. Bei vielen Anbietern ist beispielsweise festzustellen, dass sie während der Konferenz anfallende personenbezogene Daten auch für eigene Zwecke oder für Zwecke Dritter nutzen, obwohl die hierfür notwendige Rechtsgrundlage für die damit verbundene Offenlegung der Daten regelmäßig schwierig zu begründen ist. Eine Untersuchung zahlreicher Videokonferenzdienste durch die Berliner Beauftragten für Datenschutz und Informationsfreiheit[21] im Juli 2020 hatte dies in vielen Fällen bestätigt. In dem auch für dieses Betriebsmodell abzuschließenden Auftragsverarbeitungsvertrag ist daher sicherzustellen, dass der Anbieter die personenbezogenen Daten der teilnehmenden Personen nur auf Weisung des Verantwortlichen und nicht für eigene Zwecke verarbeitet. Darüber hinaus sind die Verantwortlichen zur Datensparsamkeit verpflichtet. Es dürfen nur die personenbezogenen Daten verarbeitet werden, die zur Zweckerreichung auch wirklich erforderlich sind. Dieser Grundsatz ist bereits bei der Auswahl, aber auch bei der Einrichtung und dem Betrieb eines Videokonferenzsystems zu beachten.
Wir halten den Betrieb eines Videokonferenzdienstes durch den Verantwortlichen selbst oder auf einer durch einen Auftragsverarbeiter bereitgestellten Plattform für die datenschutzrechtlich vorzugswürdige Variante, denn hier kann der Verantwortliche die Umstände der Verarbeitung vollumfänglich selbst bestimmen. Gerade in größeren Unternehmen mit entsprechendem IT-Knowhow oder in den öffentlichen Verwaltungen, die auf kommunale oder landeseigene Rechenzentren zurückgreifen können, sollte ein selbst betriebenes System der Standardfall sein. Bei der Planung solcher Konferenzsysteme muss der Grundsatz der digitalen Souveränität, siehe hierzu auch Punkt 4.3.4, berücksichtigt werden. Dies führt in der Regel zum Einsatz von Open-Source-Produkten. Erfreulicher Nebeneffekt solcher Produkte sind die meist überschaubaren Kosten, denn viele Videokonferenzsysteme sind als kostenlose Open-Source-Anwendungen verfügbar und sollten den notwendigen Anforderungen gerecht werden. Auch unsere Behörde hat sich aus den genannten Gründen dazu entschlossen, ein eigenes Videokonferenzsystem auf Basis von Open-Source-Software aufzusetzen und zu betreiben.
Um Unternehmen, Behörden oder sonstigen Organisationen bei der Umsetzung der teils recht komplexen datenschutzrechtlichen Anforderungen an die Durchführung von Videokonferenzen zu unterstützen, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder die „Orientierungshilfe Videokonferenzsysteme[22]“ veröffentlicht. Adressaten sind sowohl Verantwortliche, die einen Videokonferenzdienst selbst betreiben oder von einem Dienstleister betreiben lassen, als auch Nutzer von solchen Videokonferenzsystemen, die als Online-Dienste angeboten werden. Zur Orientierungshilfe gehört eine Checkliste[23], in der die rechtlichen und technischen Anforderungen an die Videokonferenzsysteme in einer übersichtlichen und kurzen Form zusammengefasst werden.

Wir empfehlen den Verantwortlichen in Wirtschaft und Verwaltung, bei der Auswahl und beim Betrieb von Videokonferenzsystemen die Empfehlungen der „Orientierungshilfe Videokonferenzsysteme“ zu berücksichtigen.

[21] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf
[22] https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/OH-Videokonferenzsysteme.pdf
[23] https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/Checkliste-OH-Videokonferenzsysteme.pdf

5.2 Corona-Fragebogen vor Gerichtszutritt im Amtsgericht Greifswald

Im Mai 2020 erreichte uns eine Beschwerde über eine Verwaltungspraxis bei dem Amtsgericht Greifswald während der Corona-Pandemie. Das Gericht hatte festgelegt, dass vor Zutritt zum Gericht eine Selbstauskunft im Rahmen einer Beantwortung eines Besucherfragebogens zu erteilen ist. Mit den Gesundheitsfragen aus dem „Fragebogen für den Zutritt zu dem Amtsgericht Greifswald für die Dauer der Pandemie des Coronavirus (SARS-CoV-2)“ erhob das Gericht Gesundheitsdaten i. S. v. Art. 4 Nr. 15; 9 Abs. 1 DS-GVO.
Gesundheitsdaten genießen nach Art. 9 Abs. 1 DS-GVO einen besonderen Schutz. Die Verarbeitung von Gesundheitsdaten ist nach Art. 9 Abs. 1 DS-GVO untersagt, soweit nicht eine Rechtsgrundlage nach Art. 9 Abs. 2 DS-GVO die Datenverarbeitung erlaubt.
In dem Formular „Datenschutzhinweise im Zusammenhang mit der Verarbeitung von personenbezogenen Daten bei der betroffenen Person gem. Art. 13 DS-GVO für die Dauer der Pandemie des Coronavirus“ wurde als Rechtsgrundlage Art. 9 Abs. 2 lit. f und Art. 9 Abs. 2 lit. i DS-GVO angegeben.
Wir haben dem Amtsgericht mitgeteilt, dass beide Vorschriften hier nicht einschlägig sind.
Nach Art. 9 Abs. 2 lit. f DS-GVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, soweit sie „bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich“ ist. Die Vorschrift erlaubt es den Gerichten, solche sensiblen Daten insoweit zu verarbeiten, als es im Rahmen der Urteilsfindung zwingend notwendig ist. Dies können etwa Gesundheitsdaten zur Berechnung von Schadensersatzansprüchen oder zur Feststellung von sozialrechtlichen Ansprüchen sein.
In dem oben bezeichneten Formular gab das Gericht als Zweck der Datenverarbeitung aber selbst an, dass die Datenverarbeitung dem Schutz vor einer Corona-Infektion dienen sollte. Zudem erfolgt die Datenverarbeitung im Rahmen der Zugangskontrolle zum Gericht. Die Datenverarbeitung diente daher der Wahrnehmung allgemeiner Verwaltungsaufgaben und erfolgt nicht im Rahmen der justiziellen Tätigkeit. Die Datenverarbeitung ist insbesondere nicht zur Urteilsfindung erforderlich gewesen.
Art. 9 Abs. 2 lit. i DS-GVO verlangt, dass die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich ist. Damit handelt es sich bei Art. 9 Abs. 2 lit. i DS-GVO um eine sogenannte Spezifizierungsklausel. Art. 9 Abs. 2 lit. i DS-GVO legitimiert selbst die Datenverarbeitung noch nicht, sondern eröffnet dem nationalen Gesetzgeber die Möglichkeit, ein entsprechendes Gesetz zu den genannten Zwecken zu erlassen.
Ein entsprechendes Gesetz war in dem Informationsformular nicht benannt. Insbesondere handelt es sich bei den „Empfehlungen zu Arbeitsschutz- und Hygienestandards in der Landesregierung M-V“ nicht um ein entsprechendes Gesetz, das zur Datenverarbeitung befugt. Diese Empfehlungen können allenfalls bei der Beurteilung der Erforderlichkeit eine Rolle spielen. So hatten wir beispielsweise keine Bedenken gegen die Erhebung der Kontaktdaten der Besucher. Zwar ergibt sich die Zulässigkeit hier nicht aus der Verordnung der Landesregierung zur Änderung der Verordnung zum dauerhaften Schutz gegen das neuartige Coronavirus in Mecklenburg-Vorpommern in der jeweils aktualisierten Fassung. Nach § 4 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) ist aber eine Datenverarbeitung zulässig, soweit sie der Erfüllung einer Aufgabe dient, die dem Verantwortlichen übertragen worden ist.

Hier können die Empfehlungen herangezogen werden, um die Erforderlichkeit der Erhebung der Kontaktdaten zu begründen. Das DSG M-V enthält jedoch keine Regelung zur Verarbeitung von Gesundheitsdaten.
Für uns war auch kein nationales Gesetz ersichtlich, das die Gerichte in Mecklenburg-Vorpommern zur Erhebung von Gesundheitsdaten im Rahmen der Zugangskontrolle zu den Gerichten befugt.
Nachdem wir dem Gericht unsere Rechtsauffassung mitgeteilt haben, hat das Amtsgericht diese berücksichtigt und den Fragebogen ab dem 17. Juni 2020 angepasst.

5.3 Corona Beacons - Doctorbox App

Im Rahmen der Bekämpfung der Corona-Pandemie erreichte uns eine Anfrage der Landesregierung in Bezug auf die Wirtschaftsinitiative „Intelligentes Treffpunkt Management“.
Hierbei sollen in öffentlichen Einrichtungen sogenannte Beacons (engl. Funkbake oder Leuchtsignal) aufgestellt werden, welche dann regelmäßig Signale per Bluetooth aussenden. Diese Beacon-Signale können von Smartphones mit einer Bluetooth-Schnittstelle erfasst und ausgelesen werden. Die Signale sollen die jeweiligen Adress- und Positionsdaten des ausstrahlenden Beacons enthalten und beim Empfänger zusammen mit der Uhrzeit in einer freiwillig verwendeten Kontakttagebuch-App, in dem Fall der Doctorbox-App, gespeichert werden. Somit ist in der App digital hinterlegt, wo und wann sich die Nutzenden in Reichweite solcher Beacons aufgehalten haben. Die Reichweite solcher Beacons reicht dabei, in Abhängigkeit vom Aufstellort und dem Modell, von einigen wenigen bis maximal einhundert Metern.
Die Idee hinter der Kontakttagebuch-App ist dabei, dass die Daten ausschließlich lokal auf dem Endgerät, also dem Smartphone, verschlüsselt gespeichert und nicht an Dritte übermittelt werden. Die Funktionsweise ähnelt der offiziellen Corona-Warn-App der Bundesregierung, die ebenfalls eine lokale Speicherung von Daten durchführt, die per Bluetooth erfasst werden. Der Unterschied besteht dabei jedoch darin, dass hier keine Daten von anderen Personen erfasst werden, mit denen Nutzende in Reichweite getreten sind, sondern „lediglich“ der besuchte Ort. Sobald es Meldungen über Orte mit bekannt gewordenem Infektionsgeschehen gibt, würden diese mit der entsprechenden Uhrzeit an die Endgeräte aller teilnehmenden Nutzenden ausgesendet und dort lokal auf den Endgeräten mit den tatsächlich besuchten Orten abgeglichen werden. Sofern sich Nutzende zur betreffenden Uhrzeit an einem „infiziert“ gemeldeten Ort aufgehalten haben, würde diese dann eine entsprechende Meldung erhalten und könnten somit weitere Schritte einleiten.
Wir haben der Landesregierung mitgeteilt, dass wir keine datenschutzrechtlichen Bedenken gegen einen Einsatz der Beacons unter der Voraussetzung haben, dass technisch auch wirklich sichergestellt ist, dass keine personenbezogenen Daten das Endgerät verlassen, diese nach dem Stand der Technik verschlüsselt abgesichert werden und eine Nutzung der App freiwillig erfolgt. Andernfalls bestünde die Gefahr, dass ein komplettes Bewegungsprofil der Nutzenden erstellt werden könnte. Eine eigene detaillierte technische Prüfung konnte von uns mangels Personalressourcen nicht vorgenommen werden.

5.4 Corona-Listen

Nach der ersten Welle der Corona-Pandemie mit zahlreichen Schließungen kehrte das öffentliche Leben langsam wieder zurück und viele Betriebe und öffentliche Einrichtungen durften wieder öffnen. Mit viel Kreativität und Willenskraft zeigten die Unternehmen und Einrichtungen in Mecklenburg-Vorpommern, wie sie einerseits dazu beitragen wollten, das Infektionsgeschehen einzudämmen, andererseits Mitarbeiterinnen und Mitarbeiter sowie Kundinnen und Kunden zu schützen und gleichzeitig das Unternehmen und soziale und kulturelle Angebote zu retten.
Um Infektionsketten und Ausbrüche von SARS-CoV-2 (Covid-19) schnellstmöglich zu erkennen und einzugrenzen, mussten etwa Frisöre, Kosmetikstudios, aber auch Gaststätten und Cafés die Besuche ihrer Gäste oder Kunden dokumentieren. Gleiches galt auch für Angebote und Einrichtungen der Jugendarbeit, Jugendverbandsarbeit und Jugendsozialarbeit.
Große Unsicherheit und Verwirrung gab es bei den Verantwortlichen bezüglich der datenschutzkonformen Durchführung der Dokumentationspflicht. Das lag zum einen an den zunächst unklaren Vorgaben zur Dokumentation von Kontaktdaten und zum anderen waren zahlreiche Formulare im Umlauf, die jedoch nicht den Vorgaben in Mecklenburg-Vorpommern entsprachen.
Auf der Internetseite des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern wurden deshalb Hinweise zur datenschutzkonformen Kontaktdatenerhebung bereitgestellt und es wurden auch Muster für die Kontakterhebung zum Download angeboten. Um eine größtmögliche Streuweite zu erreichen, wurde auch ein datenschutzkonformes Formular über den Deutschen Hotel- und Gaststättenverband/Landesverband Mecklenburg-Vorpommern publiziert.
Trotzdem erreichten uns zahlreiche Beschwerden zum Umgang mit der Erfassung von Kontaktdaten. Bei den Beschwerden handelte es sich zumeist um offen einsehbare Kontaktlisten, übermäßige Kontaktdatenerhebung und die Nutzung von Kontaktdaten für andere Zwecke. Die Verantwortlichen wurden in den Fällen angeschrieben und um eine Stellungnahme gebeten. Die Verantwortlichen zeigten sich zum größten Teil kooperationsbereit und stellten die Kontaktdatenerfassung kurzfristig datenschutzkonform um.
Die hohe Unsicherheit bei den verantwortlichen Stellen veranlasste den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zu anlassunabhängigen und anlassbedingten stichprobenartigen Kontrollen von Unternehmen. Dabei zeigte sich, dass bei vielen Unternehmen die Kontaktdatenerfassung bereits datenschutzkonform erfolgt. Bei anderen Unternehmen wurden Hinweise gegeben, die zu einer datenschutzkonformen Kontaktdatenerfassung führten.

5.5 Unsicherheiten der Sportvereine beim Umsetzen der Auflagen der Corona-Landesverordnung Mecklenburg-Vorpommern

In der Mitte des Jahres 2020 kamen bei Sportvereinen vermehrt Unsicherheiten in Bezug auf die Umsetzung der Corona-Vorgaben des Landes auf. In einem Fall zum Beispiel wurde berichtet, dass der Sportverein zur Nutzung der städtischen Sporteinrichtungen, Sportplätze und Hallen von der Stadt angewiesen worden sei, ein Hygienekonzept vorzulegen. Hierzu seien dem Verein Listen zur Verfügung gestellt worden, in die sich Teilnehmer, Besucher und Gäste einzutragen hatten. Diese Listen seien vier Wochen aufzubewahren und dann zu vernichten. Bei einem Fußballverein zum Beispiel würden in diesem Zeitraum sehr viele personenbezogene Daten gesammelt werden.

Es wird bemängelt, dass es seitens der Stadt keine weiteren Unterweisungen und Vorgaben zum Umgang und zur Aufbewahrung dieser Daten gegeben hätte. Insbesondere die Vorgabe, dass eine Liste zu führen sei, führte in Bezug auf die datenschutzrechtliche Handhabung dieser Listen zu vielen unbeantworteten Fragen.
Weiterhin wurde kritisiert, dass die Verantwortung hier auf die unterste Ebene abgegeben werde, was zudem Kosten verursache und einige Vereine auch überfordere, zumal es mitunter auch schwierig sei, Personen zu finden, die ohne entsprechende Kenntnisse oder Einweisung solch eine verantwortungsvolle Aufgabe übernehmen möchten. Gerade bei kleinen Sportvereinen oder Sportgruppen würde für diese Fragen kein Datenschutzbeauftragter zur Verfügung stehen.
Es sei insgesamt der Eindruck entstanden, dass die Verwaltungen der Kommunen angesichts der ständig neuen Vorschriften überfordert seien und dementsprechend für die Umsetzung der gesetzlichen Vorschriften bzw. die Handhabung damit einhergehender datenschutzrechtlicher Belange und Vorgaben den Vereinen nicht beratend zur Seite stehen. Vor diesem Hintergrund werden die von der Landesregierung erlassenen Vorschriften kritisch gesehen bzw. detailliertere Vorgaben in Bezug auf die Umsetzung gefordert.

Wir empfehlen der Landesregierung bei der Gestaltung künftiger Regelungen in Bezug auf die Corona-Pandemie, die bisherigen Erfahrungen und Probleme bei der Umsetzung datenschutzrechtlicher Belange in den Blick zu nehmen, sodass die Kommunen auch die Verantwortlichen und Betreiber von Einrichtungen und Sportstätten angemessen unterstützen können.

5.6 Corona-Montagsspaziergang

Am 25. Mai 2020 fand in Rostock auf der Kröpeliner Straße eine als „Montagsspaziergang“ bezeichnete Veranstaltung statt, die Anlass für einen Polizeieinsatz war. Im Anschluss an diese Veranstaltung gingen bei uns mehrere Beschwerden ein. Als Anlage zur Beschwerde wurde auch ein Artikel aus der Ostseezeitung über diese Veranstaltung übersandt.
Ausweislich des Berichts in der Ostseezeitung vom 27. Mai 2020 demonstrierten knapp 200 Teilnehmende gegen Einschränkungen aufgrund der Corona-Pandemie. Die Demonstration war zwar angekündigt, aber nicht angemeldet.
Bereits im Vorfeld soll es zu sogenannten Montagsspaziergängen gekommen sein, die ebenfalls nicht als Demonstration angemeldet waren. Diese habe die Polizei aber geduldet.
Die Demonstranten, darunter auch Familien mit Kindern, seien von der Polizei eingekesselt worden. Demonstranten haben gegenüber der Ostseezeitung angegeben, dass sie dadurch den Mindestabstand von 1,5 m nicht einhalten konnten. Zudem gaben zwei der Beschwerdeführer an, dass sie lediglich Einkäufe in der Kröpeliner Straße tätigen wollten und sich nicht an dem Montagsspaziergang beteiligt hätten. Alle Beschwerdeführer durften den Platz erst nach einer Identitätsfeststellung verlassen.
Nach Angaben der Beschwerdeführer und dem Bericht der Ostseezeitung erfolgte die Identitätsfeststellung jedenfalls bei einem Teil der Demonstranten in der Weise, dass sich die Demonstranten vor einer weißen Hauswand aufstellen und ihren Personalausweis mittig vor die Brust halten mussten. So wurden die Demonstranten und möglicherweise auch die Passanten, die sich lediglich zufällig in der Kröpeliner Straße aufgehalten haben, dann durch Polizeibeamte des Polizeipräsidiums Rostock fotografiert.
Wir haben das Polizeipräsidium Rostock zunächst um Stellungnahme zu dem uns angezeigten Sachverhalt gebeten.

Das Polizeipräsidium Rostock hat daraufhin den von den Beschwerdeführern vorgetragenen Sachverhalt eingeräumt und ergänzend vorgetragen, dass bei den Teilnehmenden der Demonstration ein Anfangsverdacht wegen eines erheblichen vorsätzlichen Verstoßens gegen die Corona-Übergangs-Landesverordnung Mecklenburg-Vorpommern (Corona-Übergangs-LVO MV) bestanden hätte. Daher sei bei den Teilnehmenden eine Identitätsfeststellung und die Aufnahme einer entsprechenden Ordnungswidrigkeitenanzeige erforderlich gewesen. Es sei darüber hinaus auch erforderlich gewesen, die Personen bis zum Abschluss der jeweils individuellen Identitätsfeststellung vor Ort festzuhalten. Für diesen polizeilichen Gewahrsam habe eine richterliche Anordnung vorgelegen. Zur Feststellung der Identität sei eine Bearbeitungsstrecke vor Ort errichtet worden. Dies habe etwa 20 bis 30 Minuten in Anspruch genommen, während dieser Zeit seien jedoch schon mehrere Identitäten schriftlich festgestellt worden. In dieser Bearbeitungsstrecke seien zunächst die Personalien weiterhin schriftlich aufgenommen und mit dem Fahndungsbestand abgeglichen worden. Da sich jedoch herausgestellt habe, dass auf diesem Wege die Feststellung aller Personalien mehrere Stunden in Anspruch nehmen könnte, habe man sich dazu entschieden, die Personen mit den Personalausweisen zu fotografieren. Teilweise hätten die Demonstranten diese von der Polizei ergriffene Maßnahme zur Beschleunigung des Verfahrens begrüßt. Das Polizeipräsidium Rostock konnte jedoch keine Angaben dazu machen, welche oder wie viele Personen tatsächlich mit dieser Form der Identitätsfeststellung einverstanden waren.
Im Nachgang des Einsatzes sollen die Personalien anhand der Fotoaufnahmen tabellarisch erfasst und später zur aufgenommenen Ordnungswidrigkeitenanzeige hinzugefügt worden sein. Im Anschluss daran seien die gefertigten Fotos sofort gelöscht worden. Die Löschung der Fotos wurde am 4. Juli 2020 bestätigt. Fotoaufnahmen von 45 Personen hätten jedoch nicht gelöscht werden können, weil sich diese Fotoaufnahmen zusammen mit vorherigen Videoaufnahmen auf einem Datenträger befunden hätten. Diese Videoaufnahmen seien zur Beweissicherung erforderlich. Aus diesem Grund habe die sachbearbeitende Dienststelle auf dem Vorblatt der Urkopie dieses Datenträgers einen Sperrvermerk für die nicht mehr benötigten Fotoaufnahmen angebracht. Da dieser Datenträger als Beweismittel in einem Strafverfahren diene, sei dieser der KPI Rostock übergeben worden.
Die Erstellung von Lichtbildern der betroffenen Personen sowie das Abfotografieren der Personalausweise und die sich daran anschließende Datenverarbeitung verstieß nach unserer rechtlichen Bewertung gegen § 47 Nrn. 1, 3 Bundesdatenschutzgesetz (BDSG) und gegen § 25a Abs. 1 Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V).
Diese rechtliche Einschätzung hat auch das Polizeipräsidium Rostock eingeräumt. In einer anschließenden persönlichen Beratung mit Vertretern des Polizeipräsidiums Rostock wurde der rechtliche Vorwurf aus dem Anhörungsschreiben erörtert. Die Vertreter des Polizeipräsidiums Rostock räumen ein, dass bei einer ex post-Betrachtung die Vorwürfe zutreffend sein könnten, verwiesen aber zugleich darauf, dass das Ministerium für Inneres und Europa Mecklenburg-Vorpommern derzeit an der Einführung einer Anwendung arbeitet, die unter anderem der Überprüfung von Ausweisdokumenten und deren Ablichtung dienen soll. Weiterhin sei das Einsatzgeschehen kritisch und schwer überschaubar gewesen. Der Verdacht, dass die Demonstrationsteilnehmer auch gegen Straftatbestände verstoßen haben könnten, sei vor Ort nicht auszuschließen gewesen.
Nach diesem Gespräch haben wir uns mit dem Polizeipräsidium Rostock darauf verständigt, von einer Verwarnung abzusehen. Wir haben aber den Hinweis nach Art. 58 Abs. 1 lit. d DS-GVO i. V. m. § 48b Abs. 1 SOG M-V ausgesprochen und festgestellt, dass die Datenverarbeitung bei dem Einsatz nicht datenschutzkonform war.

Wir empfehlen, dass die Polizei bei der Überprüfung von Ausweisdokumenten künftig keine Fotos der Ausweise anfertigen sollte.

6 Datenschutz und Bildung

6.1 Datenschutz und die Förderung von digitalen Kompetenzen

Nach dem Willen des europäischen Gesetzgebers ist die Sensibilisierung und Aufklärung der Bürgerinnen und Bürger für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten eine zentrale Aufgabe des Landesbeauftragten für Datenschutz Mecklenburg-Vorpommern als Datenschutzaufsichtsbehörde. Art. 57 Abs. 1 lit. b DS-GVO hebt in diesem Zusammenhang ausdrücklich die Notwendigkeit spezifischer Maßnahmen für Kinder hervor. Erwägungsgrund 132 führt weiterhin aus, dass jede Datenschutzaufsichtsbehörde Sensibilisierungsangebote auch an Personen im Bildungsbereich adressieren soll.
Die Sensibilisierung zum Umgang mit den eigenen Daten, Persönlichkeitsrechten sowie die Wahrung der Rechte anderer sind unerlässlich. Dafür ist es notwendig, die Mechanismen und Funktion unserer digitalen Kultur zu verstehen und kritisch hinterfragen zu können. Die Reflektion unserer digitalen Gesellschaft setzt Wissen voraus, wie weltweit agierende Unternehmen personenbezogene Daten der Bürgerinnen und Bürger aus- und verwerten, um das Grundrecht auf informationelle Selbstbestimmung umsetzen zu können. Die Konsequenzen des Verlusts der Privatsphäre sowie ethische Fragestellungen beurteilen zu können, ist Basis für eine demokratische Kultur. Es ist erforderlich, die Vor- und Nachteile der digitalen Kultur zu kennen, um sich selbstbestimmt bewegen zu können.
Unsere Behörde verfügt über jahrelange Erfahrung in diesem Bereich. Bereits seit 2012 stellen wir umfassende landesweite Bildungsangebote für Eltern, Kinder und im Bildungsbereich tätige Personen zur Verfügung, die für den Umgang mit personenbezogenen Daten sensibilisieren und über Rechte im Zusammenhang mit der Datenverarbeitung aufklären. Dabei liegt ein Fokus auf der landesweiten Vernetzung und Koordinierung von Projekten, Institutionen und Einrichtungen sowie medienpädagogisch Tätigen und nachfragenden Zielgruppen. In diesem Sinne haben wir auch das Medienscouts MV-Projekt ins Leben gerufen und führen es als Gemeinschaftsprojekt, ein Projekt aus Mecklenburg-Vorpommern, das bundesweit Beachtung findet, siehe Punkt 6.2.
Unsere Behörde hat neue Formate und Methoden ausprobiert, um weiterhin die Aufgaben nach Art. 57 DS-GVO umsetzen zu können. Dazu gehörten digitale Fortbildungen, Expertengespräche und Vorträge. Die größte Nachfrage kam aus der Zielgruppe der Lehrkräfte und der Sozialarbeitenden. Wir haben den digitalen Medienbildungstag 2020 des Ministeriums für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern unterstützt.
Gleichzeitig sehen wir, dass die Gruppe der Kinder und Jugendlichen die geringsten Möglichkeiten hatte, an Projekten, beispielsweise Medienscouts MV, TEO - Mein Klick - meine Verantwortung, Jugend hackt, Hello World, teilzunehmen. Dazu kommt, dass nicht allen Schülerinnen und Schülern die gleichen Möglichkeiten des Distanzlernens zur Verfügung standen und stehen.
Durch die Corona-Pandemie hat sich das Verständnis für die Wichtigkeit der Förderung von Medienkompetenz/Digitaler Kompetenz erhöht, was wir begrüßen. Nach unserer Auffassung ist die Vermittlung von Datenschutzbewusstsein und Medienkompetenz/Digitaler Kompetenz weiterhin eine notwendige Zukunftsaufgabe unseres Landes.

Wir empfehlen der Landesregierung, die Vermittlung von Medienkompetenz/Digitaler Kompetenz entlang der gesamten Bildungskette prioritär zu behandeln, um allen Bürgerinnen und Bürgern die Teilhabe an unserer digitalen Kultur zu ermöglichen.

6.2 Medienscouts MV und TEO – Tage ethischer Orientierung - protect privacy

Medienscouts MV - Jugend klärt auf

Das Projekt der Medienscouts MV[24] war im Berichtszeitraum ebenso geprägt von den Auswirkungen der Corona-Pandemie wie alle anderen Bildungsprojekte. So musste das für den 20. bis 22. März 2020 geplante Ausbildungswochenende wegen des bundesweiten ersten Lockdowns absagt werden. Auch das Ausbildungswochenende vom 20. bis 22. November 2020 musste ausfallen. Verbunden mit der Hoffnung, dass im Juni 2021 andere Voraussetzungen vorliegen, wollen wir dann wieder in eine regelmäßige Ausbildung der Medienscouts MV starten.

Um die Vernetzung der bereits ausgebildeten und zukünftigen Medienscouts MV zu verbessern, konnten wir mit Unterstützung der Landesregierung eine Medienscouts-App entwickeln. Hier wurde ein kleines soziales Netzwerk geschaffen, wo wir mit den Medienscouts in sicherer und datenschutzkonformer Umgebung News austauschen können, über einen Messenger schreiben und Workshop-Materialien zur Verfügung stellen können. Die App wurde sowohl als web-progressiv-App als auch native App für Android und iOS entwickelt. Damit können die Jugendlichen jedes Endgerät nutzen. Die Entwicklung der App konnte zum Jahresende 2020 abgeschlossen werden.

Es ist geplant, im Jahr 2021 alle bereits ausgebildeten Medienscouts MV in das soziale Netzwerk einzuladen und dann in den folgenden Ausbildungswochenenden auch die zukünftigen Medienscouts MV mit der App zu vernetzen. Gleichzeitig bietet es uns die Chance, kleine, kurze und vor allem regelmäßige digitale Treffen mit den Jugendlichen zu arrangieren. Dies wird die Erreichbarkeit und das Gefühl der Zusammengehörigkeit verbessern. Die Medienscouts MV können sich über diese digitale Plattform selbst vernetzen und sicher kommunizieren. Damit unterstützen wir den Wunsch der Jugendlichen zur Organisation von Projekttagen und Workshops, wenn wieder regelmäßiger Präsenzunterricht stattfinden kann. Weiterhin werden wir auch hier das Durchführen von Online-Veranstaltungen üben können. Diese Erfahrungen und das Wissen werden für die Medienscouts MV auch auf ihrem weiteren Lebens- und Berufsweg hilfreich sein.

TEO - Tage ethischer Orientierung: protect privacy - mein Klick, meine Verantwortung

„Tage ethischer Orientierung“ ist ein schulkooperatives Modell der Nordkirche. Das viertägige Modul „protect privacy - mein Klick, meine Verantwortung“, das in Kooperation mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern durchgeführt wird, ist speziell für die 5. und 6. Klassen konzipiert. Die Schülerinnen und Schüler lernen Inhalte rund um Datenspuren im Netz, soziale Netzwerke, Cybermobbing, Apps, Smartphones, Handys und Computerspiele kennen und erarbeiten Möglichkeiten der reflektierten und verantwortungsbewussten Nutzung digitaler Medien. Auch Lehrkräfte der beteiligten Schulklassen sind Teilnehmende der Tage ethischer Orientierung.

[24] Das Projekt der Medienscouts MV wurde 2012 vom LfDI MV ins Leben gerufen und wird seither unterstützt von der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern (LAKOST M-V), dem Landesjugendring Mecklenburg-Vorpommern e. V. (LJR M-V), dem Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V), der Landesmedienanstalt Mecklenburg-Vorpommern (MMV) und deren Online-Selbsthilfeplattform Juuuport sowie der ComputerSpielSchule Greifswald (CSG). Weitere Informationen unter: www.medienscouts-mv.de

Es handelt sich hier ebenfalls um eines unserer Gemeinschaftsprojekte. So unterstützen uns im Rahmen dieses überregional bekannten Projektes Referentinnen und Referenten der Landeskoordinierungsstelle für Suchtthemen M-V (LAKOST M-V), des Kompetenzzentrums und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern sowie der ComputerSpielSchule Greifswald (CSG).
Leider musste auch dieses erfolgreiche Projekt im Jahr 2020 wegen der Pandemie pausieren, soll aber sobald wie möglich fortgeführt werden. Hierzu bedarf es für die bekannten außerschulischen Partner verlässlicher finanzieller und personeller Rahmenbedingungen. Interessierte können sich unter www.teoinmv.de informieren.

6.3 Medienaktiv MV

Das landesweite Netzwerk für Medienbildung in Mecklenburg-Vorpommern Medienaktiv MV wird vom Landesjugendring M-V (LJR MV), der Landeskoordinierungsstelle für Suchtthemen M-V (LAKOST M-V), dem Landeskriminalamt MV (LKA M-V), dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, der Landesmedienanstalt Mecklenburg-Vorpommern (MMV) und unserer Behörde organisiert. Seit der Gründung ist dieses Netzwerk bundesweit beispielgebend, da sich hier Suchthilfe, Jugendhilfe, Medienpädagogik, Polizei, Schule und Datenschutzbeauftragter auf Augenhöhe begegnen und in zahlreichen gemeinsamen Projekten und Veranstaltungen vernetzen und engagieren.
Die Akteurinnen und Akteure des landesweiten Netzwerkes Medienaktiv MV brachten ihre Erfahrungen und ihr Know-How für die „Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern“ ein. Das Netzwerk wird von vielen außerschulischen Partnerinnen und Partnern der Medienarbeit in Mecklenburg-Vorpommern unterstützt. Dazu gehören beispielsweise Medienwerkstätten, freie medienpädagogisch Tätige, die LAG Medien e. V., der Rat für Kriminalitätsvorbeugung M-V, die Eltern- und Schülervertretungen des Landes sowie Vereine und Verbände, beispielsweise der Unternehmerverband Mecklenburg-Vorpommern.
Normalerweise veranstaltet Medienaktiv MV zwei Fachtagungen pro Jahr mit unterschiedlichen Themenschwerpunkten. Durch die Corona-Pandemie mussten diese 2020 leider ausfallen. Jedoch konnten unsere Kapazitäten in die Planung der ersten Online-Tagung mit dem Thema „Medienkompetenz in M-V - Perspektiven aus der Praxis“ fließen, welche für Januar 2021 geplant war. Zudem konnten die Netzwerkmitglieder anderweitige Kooperationen digital fortführen. Dazu zählten vor allem digitale Fachgespräche mit pädagogischen Fachkräften, aber auch Bildungsprojekte der Medienscouts MV oder den Medienguides MV oder die Unterstützung beim Zweiten Medienbildungstag des Ministeriums für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern. Die Erfahrungen aus der Corona- Pandemie werden in die künftige Planung der Netzwerkaktivitäten aufgenommen. Dazu zählt die Umsetzung von Tagungen in Online- bzw. Hybridformaten in Abwechslung zu Präsenzveranstaltungen, sobald diese wieder möglich werden. Unsere Behörde nimmt immer wieder die koordinierende und vernetzende Stellung dabei ein.
Die Internetpräsenz des Netzwerkes ist auf www.medienaktiv-mv.de verfügbar.

6.4 Kooperationsvereinbarung zur Förderung von Medienkompetenz in M-V

Die Landesregierung Mecklenburg-Vorpommern räumt mit der „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“ der Förderung von Medienbildung und Medienkompetenz einen hohen Stellenwert ein.
„Die Landesregierung ist sich mit dem Landesbeauftragten für den Datenschutz einig, dass der Grad der Medienkompetenz seiner Bürgerinnen und Bürger über den Grad seiner Teilhabe und seiner Selbstbestimmtheit in der digitalisierten Welt entscheidet. Sie sieht daher, ebenso wie der Landesbeauftragte für den Datenschutz, die diesbezügliche lebenslange Bildung als eine Kernaufgabe an.“[25]
Mit dem Erfahrungsbericht der dritten Kooperationsvereinbarung erfolgte am 19. Februar 2019 mit dem Kabinettsbeschluss der Auftrag zur Erarbeitung einer vierten Kooperationsvereinbarung. Die bisherige Vereinbarung wurde von der Staatskanzlei des Landes Mecklenburg-Vorpommern, dem Ministerium für Inneres und Sport Mecklenburg-Vorpommern, dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, dem Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern, dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern sowie der Medienanstalt Mecklenburg-Vorpommern unterzeichnet.
Obwohl die Arbeitsgruppe der Umsetzenden und medienpädagogischen Akteure (MeKo2) nicht mehr in die Erarbeitung involviert war, konnte die Arbeitsgruppe der direkt Unterzeichnenden (MeKo 1), zu der auch unsere Behörde gehört, zu Beginn dieses Berichtszeitraumes eine Vereinbarung vorlegen. In der Sitzung Anfang März 2020 wurde jedoch eine Version vorgestellt, die ein zentralisiertes Medienkompetenzzentrum für das Land Mecklenburg-Vorpommern in Wismar beschrieb. Da dieses bisher nicht Gesprächsgegenstand in der Arbeitsgruppe war und Fragen in Bezug auf die Umsetzung und Arbeit ebenfalls nicht erklärt wurden, fand dieser Vorschlag keinen Konsens in der Arbeitsgruppe. Die Mehrheit der Unterzeichnenden stimmte nicht zu, sodass die Ressortanhörung zur „Vierten Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern“ zurückgezogen wurde.
Unsere Behörde begrüßt ausdrücklich die Fortschreibung der Kooperationsvereinbarung zur Förderung von Medienkompetenz. Dieses wichtige Instrument der Förderung von Medienkompetenz wird bundesweit geachtet. So wurde durch den Wissenstransfer unserer Behörde im Bundesland Thüringen eine ähnliche Kooperationsvereinbarung geschlossen, die dem Beispiel unseres Landes folgt.[26] „Mit dieser erfolgreichen Kontinuität nimmt Mecklenburg-Vorpommern bundesweit eine Vorreiterrolle ein“, welche von der Landesregierung bereits anerkannt wurde.[27] Gleichzeitig unterstützen wir weiterhin aktiv und kreativ den Prozess, um die Finalisierung der „Vierten Kooperationsvereinbarung des Landes Mecklenburg-Vorpommern zur Förderung von Medienkompetenz in der digitalen Gesellschaft“ schnellstmöglich abzuschließen. Unsere Behörde bringt dabei konstruktiv die fachliche Expertise bei der Vermittlung von Medienkompetenz ein und leistet einen wichtigen Beitrag zur Koordinierung und Vernetzung der entsprechenden Ressorts und Institutionen.

[25] Landtags-Drucksache 7/5665, Seite 10
[26] http://www.thueringen.de/mam/th1/tsk/medien/medienkompetenz/20170221unterzeichnete_kooperationsvereinbarung.pdf
[27] Landtags-Drucksache 7/3509 „Medienbildung Mecklenburg-Vorpommern“, S. 7

Neben den Arbeitsgruppen „AG Digitale Schule“ und „AG Frühkindliche Medienbildung“, in die unsere Behörde ihre inhaltlichen Kompetenzen einbringt, gehörte nach dem parlamentarischen Auftrag auch die Arbeitsgruppe „Landesmedienkompetenzzentrum“ dazu, die sich im Oktober 2020 gegründet hat.[28] Unsere Behörde betont dabei noch einmal, dass die flächendeckende Vermittlung von Medienkompetenz entlang der gesamten Bildungskette völlig unabhängig von der Filmförderung des Landes gesehen werden muss. Eine strukturierte Koordination von Medienkompetenzvermittlung, die auf die Bedürfnisse des Landes angepasst ist, ist seit langem eine Forderung unserer Behörde und auch des Netzwerkes Medienaktiv MV. Dabei ist unbedingt zu beachten, dass keine Parallelstruktur durch die Landesregierung aufgebaut wird, sondern die Akteure und Umsetzenden gewachsene Strukturen mitnehmen. Unsere Behörde hat bereits 2019 dazu konkrete Ideen vorgelegt, die eine dezentrale Organisation über das gesamte Bundesland hinweg garantiert und gleichzeitig auf vorhandenen Strukturen aufbaut, sodass keine Parallelstrukturen entstehen. Wir werden diese Entwicklung auch weiterhin konstruktiv und zielorientiert begleiten.

6.5 Medien und Familie

Das Thema von Medienbildung und -erziehung in den Familien beschäftigt unsere Behörde bereits seit längerer Zeit. Kinder und Jugendliche auf einen nachhaltig positiven Umgang mit digitalen Medien vorzubereiten ist eine besonders wichtige Erziehungsaufgabe und bildet das Fundament der Medienkompetenzbildung.
Die Studien des Medienpädagogischen Forschungsverbundes Südwest (mpfs) KIM und miniKIM zeigen auf, dass Kinder immer früher und mehr Medien nutzen - auch schon im Vorschul- und Kindergartenalter. Durch die Corona-Pandemie hat sich die digitale Mediennutzung der Kinder und Jugendlichen 2020 noch einmal erhöht.[29] Auf dieses veränderte Heranwachsen müssen auch die Eltern reagieren, denn oft ist die PC-, Konsolen- und Smartphonenutzung der Kinder ein Thema eines Familienstreits. Besonders Kinder unter 10 Jahren sind verstärkt in familiäre Strukturen eingebunden, sodass die Eltern als Vorbilder auch in Sachen Mediennutzung dienen und den Zugang zur digitalen Welt prägen. Um ihre erzieherische Aufgabe und Vorbildfunktion zu erfüllen, braucht es auch bei den Eltern umfangreiches Wissen zu digitalen Medien, Chancen und Risiken der digitalen Welt, aktueller Programme und Endgeräte. Eltern haben allerdings sehr unterschiedliche Meinungen, Erfahrungen und Wissensbestände zu diesen Themen.
Studien zeigen, dass das Interesse an der kindlichen Medienbildung und -erziehung mit dem Schuleintritt sinkt, während zeitgleich immer mehr Kinder auf problematische Inhalte im Netz stoßen.[30] In mehreren Urteilen der letzten Jahre wurden Eltern an ihre Pflichten erinnert und zum Beispiel zum Entzug des Zweithandys, Deinstallation von Spielen oder zur Weiterbildung angewiesen. Für eine nachhaltige, bedarfs- und interessengerechte Medienbildung der Kinder braucht es dringend Angebote für Eltern. Wenn die Erwachsenen in den Fokus der Bildungsarbeit zu digitalen Kompetenzen, Medienkompetenz und Datensicherheit rücken, wird die gesamte Familie gestärkt.

[28] Landtags-Drucksache 7/5301: Konzept zur Errichtung Landesmedienkompetenzzentrum
[29] https://www.mpfs.de/studien/jim-studie/jimplus-2020/
[30] https://www.mpfs.de/studien/kim-studie/2018/ (S. 62-64)

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern engagiert sich bereits seit einigen Jahren zum Thema „Medien und Familie“ (siehe Dreizehnter Tätigkeitsbericht, Punkt 4.1.4) und sieht ein großes Potenzial für die Vermittlung von Medienkompetenz und Datenschutzbewusstsein durch die Stärkung der Eltern. Aus diesem Grund führt unsere Behörde sowohl in Kindertageseinrichtungen als auch Horten immer wieder Elternabende durch, um auf die Notwendigkeit der Medienbildung und -erziehung innerhalb der Familien hinzuweisen.

6.5.1 Medienguides Mecklenburg-Vorpommern

Wir wollen mit diesem Projekt eine Lücke im Bildungsangebot füllen und auch Eltern Angebote zur Medienkompetenz/Digitaler Kompetenz machen.
Andere Bundesländer haben schon niedrigschwellige Angebote wie „ElternTalks“ eingeführt, die direkten Nachbarn Hamburg und Schleswig-Holstein führen mit den „ElternMedienLotsen“ ebenfalls ein peer-to-peer-Projekt durch.
In Anlehnung an das erfolgreiche Medienbildungsformat unserer Behörde „Medienscouts MV - Jugend klärt auf“ sollte die Zielgruppe in 2020 auf die Elterngeneration ausgeweitet werden. Beim neuen Projekt „Medienguides MV“ wollen wir zunächst Eltern von Kindern bis zur 6. Klasse eine vielseitige Ausbildung anbieten sowie das methodische Wissen, das die Eltern dann ebenfalls mit anderen Eltern teilen. Die Konzeptidee der Medienguides MV beruht ebenso auf dem peer-to-peer-Ansatz. Durch die Corona-Pandemie startete die Planung und Umsetzung des Projektes Medienguides MV erst im Herbst 2020.
Um Synergien zu nutzen, wird das Medienguides MV-Projekt durch die Projektpartner des Medienscouts MV-Projektes und weitere Institutionen aus dem Netzwerk Medienaktiv MV in der Planung unterstützt. Bis Ende 2020 konnte unsere Behörde bereits einige engagierte Institutionen gewinnen und inhaltliche Schwerpunkte zusammen erarbeiten. Gemeinsam werden im Frühjahr 2021 die Präsentation und der Ablauf für den Pilotdurchlauf im Herbst 2021 erarbeitet.
Um die konkreten Wünsche, Bedürfnisse und Motivation der Zielgruppe „Eltern“ in Mecklenburg-Vorpommern aufzugreifen, wird im Januar 2021 ein Fokusgruppentest avisiert. Die Ergebnisse der Umfrage unter Eltern in Mecklenburg-Vorpommern über die Medienbildung und -erziehung werden in unsere Planung einfließen. Diese Umfrage unter Eltern in Mecklenburg-Vorpommern ist die aktuellste Abfrage der Wünsche und Probleme in Bezug auf Medienbildung und -erziehung in unserem Land.
Das Ziel der Ausbildung soll sein, interessierte Eltern zu Themen wie sicherer Umgang mit den eigenen Daten, Einstellungen in Apps und auf Geräten sowie zu Themen wie Cybergrooming, digitale Spiele, Mediennutzungszeiten und Mobbing aufzuklären. Wir planen derzeit eine Gruppierung der Eltern nach Alter der Kinder. Da es noch nicht absehbar ist, wie sich das Pandemiegeschehen gestalten wird, beabsichtigen wir die Ausbildung analog und/oder hybrid durchzuführen. Im Fall einer weiteren bzw. andauernden Pandemiewelle ist auch die rein digitale Durchführung als Alternative zu planen, bei der Online-Quiz und Video-Tutorials eingebunden werden könnten. Der Ansatz des Projektes soll niedrigschwellig, auf Augenhöhe und bedarfsorientiert sein. Die vermittelten Inhalte und Methoden bereiten die Teilnehmenden sowohl für die Verwendung in der eigenen Familie als auch für multiplizierende Veranstaltungen mit anderen Eltern vor mit einem konstruktiven Austausch der Eltern.

Die qualifizierten Medienguides MV könnten sowohl an den Schulen und Kitas ihrer Kinder als auch an Einrichtungen ihrer Region ehrenamtlich Ansprechpersonen zu Fragen und Themen im Bereich der Medienkompetenz werden. Durch diese Weitervermittlung des Wissens im peer-to-peer-Ansatz möchten wir erreichen, dass die vermittelten Inhalte langfristig und nachhaltig bei einer Vielzahl von Familien ankommen können. Dabei können die Medienguides MV auch ihre eigenen Erfahrungen als Eltern einfließen lassen, sodass im besten Falle ein ehrlicher, praxisorientierter und lebensnaher Austausch stattfindet, der Hilfestellung für den gesamtfamiliären Medienkonsum bietet. Materialien und Methodentipps sollen den künftig teilnehmenden Eltern auch digital zur Verfügung gestellt werden. Denkbar wären eine eigene Website und eine App, wie sie auch das Jugendprogramm „Medienscout MV“ nutzt. In der weiteren Planung sollen die Medienguides MV-Seminare zur Vernetzung, thematischen Vertiefung oder Auffrischung bereitgestellt werden. Im Laufe der ersten Jahreshälfte 2021 sind weitere Informationen zum Projekt auf der Website unserer Behörde und auf einer eigenen Projektseite zu finden.

6.5.2 Neues Kapitel Bildungskonzeption der 0- bis 10-Jährigen in Mecklenburg-Vorpommern

Im Dreizehnten Tätigkeitsbericht haben wir bereits unter Punkt 4.1.3 über die Arbeitsgemeinschaft „Frühkindliche Medienbildung“ berichtet, die aus der „Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern“ hervorgegangen ist. Seit diesem Zeitpunkt hat unsere Behörde ihre fachliche Expertise in die Erarbeitung des Kapitels „Medien und digitale Bildung“ für die aktualisierte „Bildungskonzeption der 0- bis 10-Jährigen in Mecklenburg-Vorpommern“ (BiKo M-V) vorangetrieben und eingebracht. Die Federführung der Arbeitsgruppe lag beim Ministerium für Soziales, Integration und Gleichstellung Mecklenburg-Vorpommern.
Die Vermittlung von Medienkompetenz im frühkindlichen Bereich ist mit dem neuen Kindertagesförderungsgesetz Mecklenburg-Vorpommern (KiföG M-V) im Januar 2020 verpflichtend geregelt worden. Die aktualisierte Fassung mit dem beschriebenen neuen Kapitel ist in der „Bildungskonzeption der 0- bis 10-Jährigen in Mecklenburg-Vorpommern“ geregelt und wird im Februar 2021 veröffentlicht. Damit ergibt sich ein neuer Fort- und Weiterbildungsbereich für die Erzieherinnen, Erzieher und Träger im Land. Diese Möglichkeit bietet der modulare Fortbildungskurs „klicken, spielen, zappen“, der jedoch noch nicht verstetigt ist, siehe Punkt 6.5.3.
Unsere Behörde engagiert sich seit Jahren für die Vermittlung von Medienkompetenz bereits im Kita- und Grundschulalter. Das beinhaltet alle Ebenen, also Fort- und Weiterbildung der pädagogischen Fachkräfte, spezielle Angebote für Kinder sowie vor allem auch die Elternarbeit.

6.5.3 Fortbildungsreihe „klicken, spielen, zappen“

Aus der Kampagne „Medien-Familie-Verantwortung“ aus dem Herbst 2016 und der daraus resultierenden Plakatkampagne „Heute schon mit deinem Kind gesprochen“, die bundesweit ebenfalls große Beachtung fand, ist ein modulares Fortbildungsprogramm für Erzieherinnen und Erzieher entstanden.
Die Koordination des gesamten Projektes liegt bei der Landeskoordinierungsstelle für Suchtthemen (LAKOST M-V), welche zunächst nur mit unserer Behörde und später auch mit anderen Institutionen und Trägern, unter anderem aus dem Netzwerk Medienaktiv M-V, kooperierte. Die finanzielle Unterstützung durch den Verband der Ersatzkassen (vdek e. V.) ermöglichte das Fortbildungsprogramm.

Seit Januar 2018 wird jährlich eine Fortbildungsreihe für Erzieherinnen und Erzieher durchgeführt. Unsere Behörde unterstützt diese Fortbildungsreihe inhaltlich mit zwei Ganztagsmodulen. 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.[31] Dabei erfüllt der Fortbildungskurs alle wesentlichen Inhalte des im Kindertagesförderungsgesetz M-V (KiföG M-V) geregelten Bereiches der Medienbildung und Medienkompetenzvermittlung sowie des neuen Kapitels der Bildungskonzeption für 0- bis 10-Jährige in Mecklenburg-Vorpommern, siehe Punkt 6.5.2.
Nach der vielversprechenden Evaluierung der Durchläufe 2018 und 2019 ist eine Weiterführung der Kooperation ebenfalls für 2021 und 2022 finanziert. Aufgrund der Corona-Pandemie mussten die Module ab Frühjahr 2020 erst ausgesetzt und im Folgenden dann online durchgeführt werden. Der Kurs aus 2020 wird somit erst im Frühjahr 2021 seinen Abschluss finden. Die Finanzierung trägt dabei noch immer der vdek e. V. Unsere Behörde fordert seit Beginn der Fortbildungsreihe eine Verstetigung durch die Landesregierung über die LAKOST M-V.

7 Technik und Organisation

7.1 Das Standard-Datenschutz-Modell (SDM)

Die im November 2019 verabschiedete Version 2.0 des Standard-Datenschutz-Modells (SDM)[32], siehe 15. Tätigkeitsbericht Punkt 7.1.5, findet in der Landesverwaltung Mecklenburg-Vorpommerns in zunehmendem Maße Verbreitung. So werden die Prinzipien des SDM bei der Planung und Konzeption zahlreicher Fachverfahren angewendet. Auch der IT-Dienstleister der Landesverwaltung, die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, hat das SDM in sein Beratungsportfolio aufgenommen. Beispielsweise wird die Schutzbedarfsfeststellung, die bei der Erstellung eines Sicherheitskonzeptes nach der BSI-Grundschutzmethodik erforderlich ist, inzwischen standardmäßig mit der Risikoanalyse und der Schwellwertanalyse für die Datenschutzfolgenabschätzung kombiniert und das gesamte Verfahren mit Hilfe der Gewährleistungsziele des SDM strukturiert. Damit kann sichergestellt werden, dass auch die datenschutzrechtlichen Anforderungen, die über Fragen der Informationssicherheit hinausgehen, bei Verfahrensplanungen frühzeitig berücksichtigt werden.
Aber auch bundesweit findet das SDM immer mehr Zuspruch, sowohl in der Verwaltung als auch in der Wirtschaft. Uns erreichten im Berichtszeitraum zahlreiche Anfragen von kleinen Kommunen bis hin zu großen Konzernen zur Anwendung des SDM, aber auch Hinweise auf kleinere Fehler und Vorschläge zur Verbesserung des Standards. Diese Vorschläge werten wir sorgfältig aus und lassen sie nach entsprechender Prüfung in neue Versionen des SDM einfließen. Schon die im Dezember 2019 veröffentlichte Version 2.0a war eine solche fehlerbereinigte Version.

[31] Die weiteren Module werden durch LAKOST M-V, Kompetenzzentrum und Beratungsstelle für exzessiven Mediengebrauch und Medienabhängigkeit, freie Medienpädagoginnen, Medienwerkstatt raabatz der RAA Waren in der Bildungsstätte Schabernack - Zentrum für Praxis und Theorie der Jugendhilfe e. V. durchgeführt.

[32] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf

Die Version 2.0b unterschied sich von der Vorgängerversion durch Änderungen im Kapitel E6, das Hinweise zum Umgang mit dem Referenzmaßnahmen-Katalog enthält, insbesondere zum Grad der Verbindlichkeit einzelner Maßnahmen der jeweiligen Bausteine des Katalogs.
Nachdem die SDM-Methode mit der Version 2.0b inzwischen einen recht stabilen Stand erreicht hat, hat die SDM-Arbeitsgruppe des AK Technik, siehe Punkt 4.2, ihren Arbeitsschwerpunkt auf die Bereitstellung weiterer Bausteine für den Referenzmaßnahmen-Katalog gelegt. Im Berichtszeitraum wurden die Bausteine „Aufbewahren“, „Dokumentieren“, „Protokollieren“, „Trennen“, „Löschen und Vernichten“, „Berichtigen“ und „Einschränken der Verarbeitung“ veröffentlicht und zur Nutzung offiziell freigegeben. Auch zu den Bausteinen erreichten uns zahlreiche Hinweise von Anwendern des SDM. Die Bausteine mit Versionsbezeichnungen 1.0a verdeutlichen, dass die Verbesserungsvorschläge bereits zu Überarbeitungen von Bausteinen geführt haben.
Die Datenschutzaufsichtsbehörden sind gehalten, die Europäische Datenschutz-Grundverordnung (DS-GVO) einheitlich in der gesamten Union anzuwenden (Art. 51 Abs. 2). Wir sind sicher, dass das SDM einen Beitrag zur einheitlichen Anwendung der DS-GVO leisten kann. Insbesondere vor diesem Hintergrund haben wir die Version 2.0b ins Englische übersetzen lassen und in unserem Internetangebot bereitgestellt[33].

Nach wie vor aktuell ist unsere Empfehlung an die Landesregierung, bei der Einrichtung und beim Betrieb von personenbezogenen Verarbeitungstätigkeiten die im Standard-Datenschutz-Modell (SDM) beschriebene Vorgehensweise anzuwenden und das dort beschriebene Datenschutz-Management-System einzurichten.

7.2 Microsoft Office 365

Seit vielen Jahren befassen wir uns im Rahmen von Arbeitsgruppen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit Produkten der Firma Microsoft. Wir berichten seit dem Dreizehnten Tätigkeitsbericht regelmäßig darüber, zuletzt im Fünfzehnten Tätigkeitsbericht unter den Punkten 7.1.2 und 7.1.4.
In diesem Berichtszeitraum bildeten die sogenannten Online Services Terms (OSTs) in Verbindung mit dem Data Protection Addendum (DPA) der Firma Microsoft einen Arbeitsschwerpunkt. Hinter den genannten englischen Bezeichnungen verbergen sich vertragliche Regelungen für die Bereitstellung eines Clouddienstes der Firma Microsoft, der beispielsweise die Bürosoftware Microsoft 365 mit den einzelnen Anwendungen wie Word, Excel oder PowerPoint beinhaltet. Die Datenverarbeitung findet dabei nicht auf technischen Einrichtungen des datenschutzrechtlich Verantwortlichen statt, sondern auf denen der Firma Microsoft. Wird nun der oben genannte Clouddienst vom Verantwortlichen zur Erfüllung seiner Aufgaben eingesetzt, ist daher ein Vertrag nach Art. 28 Abs. 3 DS-GVO erforderlich, da der Verantwortliche personenbezogene Daten durch die Firma Microsoft im Auftrag verarbeiten lässt. Das DPA soll gemäß Microsoft den Teil der Anforderungen nach Art. 28 Abs. 3 DS-GVO abbilden. Um den Clouddienst im Wege der Auftragsverarbeitung durch den Verantwortlichen zu nutzen, ist somit sowohl der Abschluss der OSTs für die Erbringung des Clouddienstes als auch der Abschluss des DPA erforderlich, welcher die Auftragsverarbeitung durch Microsoft abbildet.

[33] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b_EN.pdf

Die Unterarbeitsgruppe „Microsoft Office 365“ des Arbeitskreises Verwaltung der DSK kam nach intensiver Befassung mit den OSTs und dem DPA (Stand: Januar 2020) zu einem Arbeitsergebnis, welches, getragen durch den AK Verwaltung, auf der 3. Zwischenkonferenz der DSK im September 2020 diskutiert wurde. Noch bevor sich die DSK im September mit dem Thema befasste, wurde das Arbeitsergebnis öffentlich bekannt und in Fachkreisen intensiv diskutiert. Dem Arbeitskreis wurde unter anderem vorgeworfen, dass er sich nicht mit den aktuellen vertraglichen Regelungen der Firma Microsoft auseinandergesetzt hätte. Dabei wurde jedoch außer Acht gelassen, dass Änderungen an den DPA ältere Verträge nicht betreffen. Denn alle abgeschlossenen DPA behalten während der Laufzeit des abgeschlossenen Onlinedienstes unverändert und vertraglich verbindlich ihre Gültigkeit. Vor diesem Hintergrund ist die Kritik des Arbeitskreises nach wie vor berechtigt.
In der 3. Zwischenkonferenz der DSK zeigte sich, dass unter den Aufsichtsbehörden kein einheitliches Meinungsbild zu den Arbeitsergebnissen des Arbeitskreises zu finden war. Neben uns unterstützten weitere acht Aufsichtsbehörden die kritische Auffassung des Arbeitskreises, die verbleibenden acht Aufsichtsbehörden lehnten einen Beschlussvorschlag des Arbeitskreises ab. Das Protokoll der 3. Zwischenkonferenz der DSK vom 22. September 2020[34] enthält in der Anlage 1 die Bewertung des AK Verwaltung vom 15. Juli 2020.
Im Ergebnis der kontroversen Diskussion wurde eine neue Arbeitsgruppe eingerichtet, die auf der Grundlage der bisherigen Ergebnisse weitere Gespräche mit Microsoft führen soll, um zeitnah datenschutzrechtliche Nachbesserungen zu erreichen. Dabei sollen auch die erforderlichen Anpassungen in Bezug auf Datenübermittlungen an Drittstaaten zur Sprache kommen, die durch die sogenannte Schrems II-Entscheidung des Europäischen Gerichtshofes (EuGH), siehe Punkt 3.6, neu bewertet werden müssen. An dieser neuen Arbeitsgruppe beteiligt sich auch unsere Behörde. Zurzeit sehen wir erheblichen Nachbesserungsbedarf bei der Ausgestaltung eines Vertrages zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO mit Microsoft als Auftragsverarbeiter.

Wir empfehlen den Verantwortlichen sowohl im öffentlichen als auch im nicht-öffentlichen Bereich, die Onlinedienste von Microsoft (z. B. die Bürosoftware Microsoft Office 365 mit Word, Excel, PowerPoint) im Rahmen der Auftragsverarbeitung bereits einsetzen oder deren Einsatz planen, zu prüfen, ob sie in der Lage sind, diese Produkte datenschutzgerecht einzusetzen. Prüfmaßstab sind die Arbeitsergebnisse des Arbeitskreises Verwaltung der Datenschutzkonferenz. Insbesondere mit Blick auf die Anforderungen zur Gewährleistung der Digitalen Souveränität empfehlen wir den Verantwortlichen den Einsatz alternativer Produkte, insbesondere aus dem Open Source Bereich, zu prüfen.

7.3 Microsoft Windows 10

Die für die Verarbeitung personenbezogener Daten Verantwortlichen, die Betriebssysteme von Microsoft verwenden, müssen prüfen, ob ihnen ein datenschutzgerechter Einsatz von Windows 10 möglich ist. Zur Unterstützung dieser Prüfung hat die Datenschutzkonferenz bereits im vorletzten Berichtszeitraum ein Prüfschema herausgegeben, siehe Fünfzehnter Tätigkeitsbericht, Punkt 7.1.2. Ergänzend dazu hat sie im letzten Jahr einen Beschluss unter dem Titel „Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise“[35] veröffentlicht.

[34] https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf
[35] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20201126_Beschluss_Telemetrie_Win10_Enterprise.pdf

Die sogenannten Telemetriefunktionen können zu einer Übermittlung personenbezogener Daten an das Unternehmen Microsoft führen. Diese Funktionen sind in einem gewissen Maß durch die Verantwortlichen konfigurierbar. Aber selbst bei der Edition Windows 10 Enterprise, die für größere Organisationen gedacht ist und bei der die Konfigurationsmöglichkeiten in diesem Punkt am weitesten ausgebaut sind, kann der Abfluss personenbezogener Daten mit Bordmitteln nicht völlig unterbunden werden. Dies zeigen insbesondere Untersuchungsergebnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die dem oben genannten Beschluss beigefügt sind.

Für Windows 10 Enterprise kommt der Beschluss daher zu dem folgenden Fazit:

„Zur Unterbindung der Übermittlung personenbezogener Telemetriedaten haben die Verantwortlichen beim Einsatz der Enterprise-Edition die Telemetriestufe Security zu nutzen und mittels vertraglicher, technischer oder organisatorischer Maßnahmen (z. B. durch eine Filterung der Internetzugriffe von Windows-10-Systemen über eine entsprechende Infrastruktur) sicherzustellen, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfindet.“
„... die bisherigen Untersuchungen [können] Verantwortliche nicht abschließend von ihrer aus Art. 5 Abs. 2 DS-GVO abzuleitenden Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten entlasten. Dies gilt erst Recht [sic] für Verantwortliche, die Windows 10 in der Pro- und Home-Edition einsetzen, in denen die Telemetriestufe derzeit nicht auf Security gesetzt werden kann. In diesen Fällen bleiben ohnehin andere Maßnahmen zur Unterbindung etwaiger Übermittlungen personenbezogener Telemetriedaten zu prüfen oder die Rechtmäßigkeit der Übermittlung nachzuweisen.“
Sollte Microsoft bei seinen Windows-Betriebssystemen auch künftig nicht die Möglichkeit bieten, die Verarbeitung von Telemetriedaten vollständig zu deaktivieren, müssen Verantwortliche dauerhaft zusätzliche vertragliche, technische oder organisatorische Maßnahmen zur Unterbindung der beschriebenen Risiken umsetzen. Alternativ kommt der Umstieg auf andere Betriebssysteme, beispielsweise aus dem Open-Source-Bereich, in Betracht. Verantwortliche müssen sicherstellen, dass auch auf der Ebene der Betriebssysteme die Anforderungen der DS-GVO vollständig umgesetzt werden, also beispielsweise unzulässige Datenübermittlungen nachweisbar unterbunden werden, und auch den Anforderungen an Digitale Souveränität Rechnung getragen wird, siehe auch Punkt 4.3.4. Gehen neue Lösungen auf Basis von Windows 10 in Betrieb, ohne dass die oben beschriebenen Risiken beherrscht werden, müssen wir uns ein Verbot gemäß Art. 58 Abs. 2 lit. f DS-GVO ausdrücklich vorbehalten.

Wir empfehlen der Landesregierung, PC-Arbeitsplätze künftig nur mit solchen Betriebssystemen auszustatten, die eine rechtmäßige Verarbeitung personenbezogener Daten erlauben (Art. 6 DS-GVO) und die es ermöglichen, die Grundsätze für die Verarbeitung personenbezogener Daten zu gewährleisten (Art. 5 DS-GVO). Bestehende PC-Arbeitsplätze müssen mittelfristig angepasst werden.

7.4 Akkreditierung und Zertifizierung nach der DS-GVO

In den Artikeln 42 und 43 der Europäischen Datenschutz-Grundverordnung (DS-GVO) werden einheitliche Akkreditierungs- und Zertifizierungsverfahren geregelt. Eine Zertifizierung nach der DS-GVO dient dazu, die Datenschutzkonformität von Verarbeitungen personenbezogener Daten sichtbar zu machen. Solche Zertifizierungen können insbesondere dann sinnvoll sein, wenn Verantwortliche über die Wahl von Dienstleistern entscheiden sollen oder um ihrer eigenen Rechenschaftspflicht in verschiedenen Konstellationen einfacher nachzukommen, siehe hierzu auch 15. Tätigkeitsbericht, Punkt 7.2.
Sofern interessierte Stellen im Datenschutzbereich Zertifizierungen vornehmen möchten, müssen sich diese im Vorfeld durch die Deutsche Akkreditierungsstelle (DAkkS), in Zusammenarbeit mit der jeweils zuständigen Aufsichtsbehörde, akkreditieren lassen. Zum Nachweis ihrer Eignung und Fachlichkeit haben sie dabei den Nachweis zu erbringen, dass sie die Anforderungen der EN-ISO/IEC 17065/2012 („Konformitätsbewertung - Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren“) erfüllen. Diese Norm enthält Grundsätze für und Anforderungen an die Kompetenz und Unparteilichkeit der Zertifizierung von Produkten (einschließlich Dienstleistungen) und Prozessen sowie der Stellen, die diese Tätigkeiten anbieten. Darüber hinaus sind aber auch die ergänzenden Anforderungen aus dem Datenschutzbereich nachzuweisen, die im Papier „Anforderungen zur Akkreditierung gemäß Art. 43 Abs.3 DS-GVO i. V. m. DIN EN ISO/IEC 17065“ definiert werden. Im Berichtszeitraum konnten diese Anforderungen zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss erfolgreich abgestimmt werden.
Um die erwähnte Zusammenarbeit zwischen den einzelnen Aufsichtsbehörden des Bundes und der Länder mit der DAkkS im Rahmen des Akkreditierungsverfahrens zu regeln, wurde im Berichtszeitraum auch eine Kooperationsvereinbarung abgeschlossen. Diese Vereinbarung regelt darüber hinaus aber auch die Möglichkeit der gegenseitigen Unterstützung der Aufsichtsbehörden untereinander, beispielsweise um bestehende personelle Engpässe in Form einer Bereitstellung von Fachpersonal zu überbrücken. Gerade mit Blick auf die Personalausstattung in unserer Behörde, siehe hierzu auch 15. Tätigkeitsbericht, Punkt 2, ist diese Regelung für uns von besonderer Bedeutung.

7.5 Apple Look Around - Kartendienst mit Speicherung personenbezogener Daten in den USA

Im August des Berichtszeitraumes erreichte uns eine Presseanfrage zu Kamerafahrten durch die amerikanische Firma Apple. Hierbei wurden mit mehreren Sensoren und Kameras ausgerüstete Fahrzeuge gesichtet, die auf öffentlichen Straßen in Mecklenburg-Vorpommern unterwegs waren. Apple selbst gibt an, dass durch Analyse von Wegen und Verkehrszeichen das Datenmaterial des eigenen Kartendienstes „Apple Maps“ verbessert werden soll. Außerdem könnten laut Apple diese Bilder der Straßen und Häuser künftig in der geplanten Funktion „Apple Look Around“ („Umsehen-Funktion“), analog dem Dienst „Google Street View“, siehe hierzu auch Zehnter Tätigkeitsbericht, Punkt 4.2.1, dargestellt und im Internet veröffentlicht werden.
Apple hat gegenüber der in Deutschland zuständigen bayerischen Datenschutz-Aufsichtsbehörde (BayLDA) bestätigt, dass die Gesichter von Personen und die Kennzeichen von Fahrzeugen vor einer Veröffentlichung automatisch verpixelt und damit unkenntlich gemacht werden sollen. Damit will Apple der Forderung der Europäischen Datenschutz-Grundverordnung (DS-GVO) nach Datenschutz durch Technikgestaltung nachkommen und die Risiken der Verarbeitung personenbezogener Daten senken.

Doch auch wenn die Gesichter und die Kfz-Kennzeichen nach Angaben von Apple vor einer Veröffentlichung verpixelt werden sollen, ist nach den bisher veröffentlichen Informationen von Apple davon auszugehen, dass die Aufnahmen in nicht unkenntlich gemachter Form („Rohdaten“) über einen Zeitraum von bis zu 36 Monaten hinweg weiter unverpixelt auf den Servern der USA vorliegen. Zudem erfordert das Unkenntlichmachen der eigenen Hausfassade, des Vorgartens oder des geparkten Autos den aktiven Widerspruch der Betroffenen.
Apple hat dem BayLDA gegenüber bestätigt, dass Betroffene die Möglichkeit haben, sich an das Unternehmen zu wenden, um zu verlangen, dass die sie betreffenden Bilder, auch in Form der Rohdaten, dauerhaft unkenntlich gemacht werden. Für diesen Fall haben wir ein entsprechendes Formular auf unserer Webseite[36] bereitgestellt.

8 Datenschutz in verschiedenen Rechtsgebieten

8.1 Parlament

8.1.1 Urteil EuGH: DS-GVO und Parlamente

Bei Wirksamwerden der DS-GVO war die Meinung weit verbreitet, dass diese Verordnung auf Parlamente im Kernbereich ihres Handelns nicht anwendbar ist. Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fasste im Jahr 2018 einen Beschluss, in dem die Auffassung vertreten wird, dass Parlamente im Kernbereich ihres Handelns nicht der DS-GVO unterfallen. Interessant ist allerdings, dass der Wissenschaftliche Dienst des Deutschen Bundestags bereits in einem am 17.08.2018 veröffentlichten Papier mit dem Titel „Sachstand Anwendbarkeit der Datenschutzgrundverordnung“ mit dem Aktenzeichen WD 3 - 3000 - 299/18 zu dem Ergebnis kommt, dass Parlamente sehr wohl der DS-GVO unterfallen.
Wichtig an dieser Diskussion ist, dass allgemein davon ausgegangen wird, dass das, was für das Parlament als Ganzes gilt, auch für seine Teile, also insbesondere die Ausschüsse und die Fraktionen, und die einzelnen Abgeordneten in ihrer parlamentarischen Tätigkeit gilt.
In einem konkreten Streitfall, in dem es um den Petitionsausschuss des Hessischen Landtags ging, musste die Frage der Geltung der DS-GVO vom Europäischen Gerichtshof entschieden werden. In seinem Urteil vom 9. Juli 2020 kommt der EuGH nach ausführlicher Darlegung der Sach- und Rechtslage zu folgendem Ergebnis:
„Art. 4 Nr. 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Europäischen Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ist dahin auszulegen, dass der Petitionsausschuss eines Gliedstaats eines Mitgliedstaats insoweit, als dieser Ausschuss allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als „Verantwortlicher“ im Sinne dieser Bestimmung einzustufen ist, sodass die von einem solchen Ausschuss vorgenommene Verarbeitung personenbezogener Daten in den Anwendungsbereich dieser Verordnung, u. a. unter deren Art. 15, fällt.“
Es ist in der Tat so, dass die DS-GVO bestimmte Bereiche der Datenverarbeitung, beispielsweise von Strafverfolgungsbehörden oder Gerichten, von der Anwendung der DS-GVO ganz ausnimmt oder Sonderregelungen verlangt. Zu diesen Ausnahmebereichen gehört die Arbeit von Parlamenten aber nicht. So heißt es im erwähnten Urteil: „… ist in der Verordnung 2016/679, insbesondere in deren 20. Erwägungsgrund und deren Art. 23, keine Ausnahme in Bezug auf parlamentarische Tätigkeiten vorgesehen.“ (Randnote 72)

[36] https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Muster/Widerspruch_DV_Apple.pdf

Dies muss dann für das Parlament als Ganzes, seine Ausschüsse, die Fraktionen und auch die einzelnen Abgeordneten in ihrer parlamentarischen Tätigkeit gelten. Ausnahmen gibt die DS-GVO offenbar nur für eng begrenzte Bereiche, etwa für die Außen- und Sicherheitspolitik, her.
Die DSK hat im Anschluss an dieses Urteil durch Beschluss vom 22. September 2020 ihren Beschluss aus 2018 ausgesetzt. Die Konferenz der Direktorinnen und Direktoren der deutschen Landesparlamente, des Deutschen Bundestags und des Bundesrats hat sich ebenfalls mit dem Urteil befasst und beschlossen, über die Auswirkungen einen Erfahrungsaustausch zu organisieren.
Zu Beschlüssen im Landtag von Mecklenburg-Vorpommern ist es zu dieser Problematik bislang nicht gekommen.

8.1.2 Verschlüsselung - gut oder gar nicht

Im November 2020 wurde der Resolutionsentwurf „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ des Rates der Europäischen Union (Nr. 12143/1/20 vom 6. November 2020) bekannt. Als Reaktion auf jüngste Terroranschläge soll Sicherheitsbehörden und Geheimdiensten die Möglichkeit eröffnet werden, auf Inhalte verschlüsselter Kommunikation zuzugreifen. Insbesondere auf Inhalte von Messenger-Diensten wie WhatsApp, Threema oder Signal, die mit einer Ende-zu-Ende-Verschlüsselung ausgestattet sind, sollen die besagten Behörden Zugriff erhalten. Die dafür erforderlichen technischen Mittel sollen in Zusammenarbeit mit den Anbietern von Online-Diensten entwickelt werden.
Die Diskussion um die Schwächung kryptographischer Verfahren wird seit mehr als 20 Jahren geführt. Im Rahmen der sogenannten Krypto-Kontroverse musste bereits vor der Jahrtausendwende befürchtet werden, dass das Recht auf Verschlüsselung eingeschränkt würde. Die Diskussion schien beendet, als sich die Bundesregierung im Juni 1999 mit den Eckpunkten der deutschen Kryptopolitik zum Einsatz kryptographischer Verfahren bekannte, siehe Vierter Tätigkeitsbericht Punkt 3.16.2. In seinem Urteil aus dem Jahr 2008 hat das Bundesverfassungsgericht (BVerfG) sogar ein neues Grundrecht abgeleitet, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Folgerichtig befürwortete die Bundesregierung im Jahr 2015 erneut den Einsatz von Kryptographie in der Charta zur Stärkung der vertrauenswürdigen Kommunikation, siehe Zwölfter Tätigkeitsbericht Punkt 4.1.10.
Doch offensichtlich fällt die europäische Politik angesichts aktueller Terroranschläge wieder in alte Muster zurück. Die europäischen Innenminister fordern unter Bezugnahme auf den Resolutionsentwurf des EU-Rates, dass die „zuständigen Behörden“ imstande sein müssten, „digitale Beweise“ im Einklang mit den Gesetzen zu sammeln und zu verwerten. Im Klartext bedeutet das, Polizei und Geheimdienste sollen Zugang zu verschlüsselten Nachrichten bekommen. Die Zusage der Innenminister, dass die Vertrauenswürdigkeit der auf der Verschlüsselungstechnologie basierenden Produkte und Dienstleistungen gewahrt bleiben muss, ist allerdings völlig unrealistisch. Denn den Fachleuten ist völlig klar: Es geht um einen General- oder Nachschlüssel zur elektronischen, verschlüsselten Kommunikation.

Hintertüren in Kommunikationsdiensten sind jedoch ein völlig untauglicher Ansatz. Wer Verschlüsselungen aufweicht, schwächt die Informationssicherheit insgesamt. Es ist aus mathematischer Sicht nicht möglich, Verschlüsselung einerseits sicher und andererseits behördlich abhörbar zu gestalten. Aus kryptographischer Sicht gibt es keine guten oder schlechten Angreifer. Vielmehr wäre ein Generalschlüssel zur Überwachung von verschlüsselter Kommunikation ein Werkzeug, von dem Kriminelle, Terroristen und Diktatoren träumen.
Im Übrigen lässt sich geheime Kommunikation weder mit einem Generalschlüssel noch mit einem Verschlüsselungsverbot wirksam verhindern. Denn die Aushöhlung von Verschlüsselungslösungen würde unweigerlich zu einem Ausweichen auf Umgehungstechniken führen, derer sich sowohl Kriminelle und Terroristen als auch technisch versierte Bürgerinnen und Bürger bedienen könnten. Allerdings würde der Einsatz wirksamer Ende-zu-Ende-Verschlüsselung für technisch weniger versierte Bürgerinnen und Bürger faktisch unmöglich gemacht.
In ihrer Entschließung vom 25. November 2020[37] ist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) den Forderungen der Regierungen der Mitgliedsstaaten der Europäischen Union entgegengetreten, Sicherheitsbehörden und Geheimdiensten die Möglichkeit zu eröffnen, auf Inhalte verschlüsselter Kommunikation zuzugreifen. Die Datenschutzkonferenz befürchtet, dass eine Schwächung der Verschlüsselungsverfahren europäische Unternehmen im globalen Markt benachteiligen könne. Die Ziele des Onlinezugangsgesetzes (OZG), Verwaltungsleistungen elektronisch über Verwaltungsportale anzubieten, würden konterkariert, wenn Nutzerinnen und Nutzer dieser Portale sich der Vertraulichkeit der elektronischen Kommunikation nicht sicher sein könnten. Sichere Ende-zu-Ende-Verschlüsselung müsse die Regel werden, um gerade im Zeitalter der Digitalisierung eine sichere, vertrauenswürdige und integre Kommunikation in Verwaltung, Wirtschaft, Zivilgesellschaft und Politik zu gewährleisten.

Wir empfehlen der Landesregierung, den Einsatz dem Stand der Technik entsprechender Verschlüsselungslösungen zu fördern und dem Bestreben, solche Lösungen zu schwächen, entschieden entgegenzutreten.

8.2 Kommunales

8.2.1 Einsicht in Bewerbungsunterlagen durch Ausschussmitglieder

Der behördliche Datenschutzbeauftragte einer Landkreisverwaltung kontaktierte uns mit der Frage, ob im Rahmen eines Stellenbesetzungsverfahrens vollständige Bewerbungsunterlagen an Mitglieder eines Fachausschusses übermittelt werden dürfen. Grundlage für dieses Ansinnen war ein Beschluss des betreffenden Ausschusses, in dem dieses eingefordert wurde.
Sowohl der behördliche Datenschutzbeauftragte als auch wir waren der Auffassung, dass die bislang praktizierte Vorgehensweise den datenschutzrechtlichen Grundsätzen sowie insbesondere den Ansprüchen des § 10 Landesdatenschutzgesetz (DSG M-V) genügt und ebenso dem Informationsinteresse der Abgeordneten entsprechen würde.

[37] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20201125_%20Ent_Schutz_vertrauliche_Kommunikation.pdf

Bislang wurden durch die Verwaltung den Ausschussmitgliedern die betreffenden vollständigen Bewerbungsunterlagen entweder zum Zeitpunkt der Sitzung oder vorher direkt bei der Verwaltung zur Einsicht bereitgestellt. Dies betraf Übersichten über die für das Stellenbesetzungsverfahren relevanten Informationen (zu den neben den stellenrelevanten Informationen insbesondere auch Angaben zum Namen, Vornamen und Wohnanschrift gehören dürften). Übereinstimmend wurde festgestellt, dass hierdurch dem für die Ausschussmitglieder geltenden Informationsrecht Rechnung getragen wird, da eine Datenübermittlung im Hinblick auf § 10 DSG M-V immer unter der Maßgabe der Erforderlichkeit erfolgen muss. Eine Übermittlung vollständiger Bewerbungsunterlagen ist nicht erforderlich. Der Begriff der Erforderlichkeit ist aus datenschutzrechtlicher Sicht eng auszulegen. Erforderlich ist eine Datenverarbeitung und somit eine Datenübermittlung nur dann, wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann.
In Hinblick darauf, dass durch dieses Verfahren insbesondere der im Art. 5 Abs. 1 lit. f DS-GVO beschriebenen Integrität und Vertraulichkeit Rechnung getragen wird, hielten sowohl der behördliche Datenschutzbeauftragte als auch wir die bisher praktizierte Vorgehensweise für richtig und lehnten eine Änderung des Verfahrens, wie vom Fachausschuss gewünscht, ab.

8.2.2 Amtsärztliche Begutachtung zur Feststellung der Fahrtauglichkeit

Ein Beschwerdeführer informierte uns darüber, dass er aufgrund einer durchgeführten Verkehrskontrolle durch die zuständige Fahrerlaubnisbehörde unter Hinweis auf Bestimmungen der Fahrerlaubnisverordnung (FEV) aufgefordert wurde, von seinem behandelnden Arzt einen Fragebogen ausfüllen zu lassen sowie anschließend beim Amtsarzt zum Zwecke einer Eignungsprüfung vorstellig zu werden. Die Rechtmäßigkeit des Verfahrens zweifelte der Beschwerdeführer uns gegenüber an.
Die Fahrerlaubnisbehörde wies in ihrer Stellungnahme darauf hin, dass im betreffenden Fall Hinweise der Polizei auf Eignungsbedenken hinsichtlich des Führens eines Kraftfahrzeuges vorlagen. Im Rahmen einer hierzu initiierten Vorprüfung wurde dem Beschwerdeführer die Möglichkeit gegeben, die Eignungsbedenken durch die freiwillige Vorlage einer ärztlichen Auskunft weitestgehend abzuschwächen. Dadurch sollte eine mögliche Gutachtenanordnung vermieden werden.
Da die Eignungsbedenken durch die freiwillig vorgelegte ärztliche Auskunft nicht ausgeräumt werden konnten, erging durch die Behörde eine Anhörung zur Vorlage eines ärztlichen Gutachtens einer amtlich anerkannten Begutachtungsstelle zur Fahreignung.
Da vorliegend Gesundheitsdaten und damit personenbezogene Daten im Sinne des Art. 9 DS-GVO verarbeitet wurden, war die datenschutzrechtliche Zulässigkeit dieser Datenverarbeitung zu prüfen. Nach Art. 9 Abs. 2 DS-GVO ist eine Verarbeitung von Gesundheitsdaten neben einer ausdrücklichen Einwilligung unter anderem auch aufgrund einer Rechtsgrundlage, die aber den Anforderungen des Art. 9 Abs. 2 lit. g) DS-GVO genügen muss, möglich. Derartige Regelungen enthält die FEV. Nach § 46 Abs. 3 i. V. m. § 11 Abs. 3 FEV kann die Fahrerlaubnisbehörde zur Prüfung der Fahreignung die Beibringung eines ärztlichen Gutachtens durch den Bewerber anordnen. Detailfragen zu dieser gesundheitlichen Betrachtung werden in den Anlagen 4 bis 6 der FEV näher beschrieben.
Das im vorliegenden Fall durchgeführte Verwaltungsverfahren entsprach den vorgenannten rechtlichen Bestimmungen, sodass aus datenschutzrechtlicher Sicht gegen diese Vorgehensweise nichts einzuwenden war.

8.2.3 Datenschutzgerechte Ausgestaltung eines Briefumschlages

Einem Wohnungsinhaber wurde zur Berechnung der Zweitwohnungssteuer von der zuständigen Amtsverwaltung postalisch ein Erhebungsbogen übermittelt. Auf dem Briefumschlag befand sich ein Stempelabdruck der vorgenannten Behörde, der neben den behördlichen und postalischen Angaben auch den Hinweis „Zweitwohnungssteuer“ enthielt. Auf einen fernmündlichen Einwand des Beschwerdeführers, dass bereits auf dem Adressstempel inhaltlich der Betreff der Korrespondenz zu lesen sei und somit gegebenenfalls datenschutzrechtliche Aspekte verletzt worden seien, wurde seitens der Verwaltung auf das bestehende Postgeheimnis sowie auf die interne organisatorische Abwicklung von Briefrückläufern verwiesen. Ein datenschutzrechtlicher Verstoß wurde dortigerseits nicht festgestellt.
Dies sahen der behördliche Datenschutzbeauftragte und wir anders, da im betreffenden Fall der in Art. 5 Abs. 1 lit. f) DS-GVO verankerte Grundsatz der Vertraulichkeit verletzt ist. Es kann nicht ausgeschlossen werden, dass der Briefumschlag mit dem infrage stehenden Stempel Dritten zugänglich gemacht wird. Aus Versehen kann beispielsweise der Brief in einen falschen Postkasten gelangen oder so hinterlegt sein, dass er für Dritte sichtbar ist. Ausgeschlossen werden kann auch nicht, dass der jeweilige Adressat beispielsweise in einer Wohngemeinschaft wohnt und damit Mitbewohner Kenntnis über den Grund des Schreibens nehmen können. In derartigen Fällen erlaubt der Briefumschlag in der derzeitigen Ausgestaltung einen Rückschluss auf den jeweiligen Inhalt.
Wir empfahlen daher eine Modifizierung des Stempels. Dies könnte beispielsweise derart erfolgen, dass statt der Bezeichnung „Zweitwohnungssteuer“ eine numerische (für Dritte nicht zuordnenbare) Bezeichnung des Fachbereichs gewählt wird.
Da der Verantwortliche der betreffenden Verwaltung trotz unserer und der Hinweise des behördlichen Datenschutzbeauftragten dieser Empfehlung bislang nicht gefolgt ist, werden weitere Schritte in dieser Angelegenheit erwogen (eine förmliche Anhörung ist bereits ergangen).

8.2.4 Sichere E-Mail-Kommunikation mit Behörden

Ein Bürger beschwerte sich über die aus seiner Sicht unsichere E-Mail-Kommunikation mit einem Landkreis. Nach unserer Bewertung des Sachverhalts bestätigte sich diese Vermutung.
Bei der Übermittlung von E-Mails sind aus datenschutzrechtlicher Sicht insbesondere die Vorgaben der Art. 5 Abs. 1 lit. f), 25 und 32 Abs. 1 DS-GVO zu erfüllen. Folglich wären Risiken, die sich bei einer Kommunikation via E-Mail ergeben, hinreichend zu mindern.
E-Mails enthalten zusätzlich zu den Inhaltsdaten (das heißt dem Text der Mail und etwaigen Anhängen) auch Metadaten wie Absender und Empfänger, das Datum und den Betreff. Sowohl Inhalts- als auch Metadaten können personenbezogene Daten beinhalten. Daher sind bei der datenschutzrechtlichen Beurteilung beide Datenarten zu berücksichtigen. Zudem erstreckt sich der gesetzlich gebotene Schutz personenbezogener Daten im Zuge der Übermittlung von E-Mail-Nachrichten auch auf die Umstände der Kommunikation, soweit sich aus letzteren Informationen über natürliche Personen ableiten lassen.

Um den oben genannten gesetzlichen Anforderungen gerecht zu werden, ist eine Verschlüsselung von E-Mails unumgänglich, wenn beispielsweise besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DS-GVO (z. B. Gesundheitsdaten) verarbeitet werden. Bei der Übermittlung von E-Mails ist grundsätzlich zwischen einer Verschlüsselung auf Inhaltsebene und einer Verschlüsselung auf Transportebene zu unterscheiden.

Inhaltsebene

Für die Verschlüsselung des Textes einer E-Mail sowie von Anhängen kommen in erster Linie die Standards S/MIME und OpenPGP infrage. Beide Standards unterstützen darüber hinaus digitale Signaturen, um Manipulationen auf dem Übertragungsweg entdecken zu können. Mit S/MIME und OpenPGP ist eine Ende-zu-Ende-Verschlüsselung möglich, das heißt, die Nachricht wird auf dem System des Absenders verschlüsselt und auf dem System des Empfängers entschlüsselt und liegt auf dem Übertragungsweg niemals im Klartext vor.
Die Metadaten werden von der Inhaltsverschlüsselung jedoch nicht erfasst, sie liegen auf den an der Übertragung beteiligten Servern im Klartext vor.

Transportebene

Bei einer Verschlüsselung auf Transportebene werden sowohl Meta- als auch Inhaltsdaten auf der Verbindung zwischen Mail-Client und Server beziehungsweise zwischen verschiedenen Mail-Servern verschlüsselt. Dadurch ist sichergestellt, dass die E-Mail während des Transports über unsichere Netze wie dem Internet von Dritten nicht mitgelesen werden kann. Auf den beteiligten Mail-Servern liegt die E-Mail jedoch im Klartext vor.
Es ist zu berücksichtigen, dass bei einer Transportverschlüsselung die E-Mails auf den E-Mail-Servern im Klartext vorliegen und grundsätzlich einsehbar sind. Bei besonders schützenswerten Daten (z. B. Kontobewegungsdaten und Gesundheitsdaten) ist eine alleinige Transportverschlüsselung daher nicht ausreichend. Zusätzliche technische und organisatorische Maßnahmen, zum Beispiel eine Ende-zu-Ende-Verschlüsselung, wären hier geboten. Sollte dies nicht gewährleistet werden können, sind gegebenenfalls alternative Übertragungswege denkbar. Hierzu zählen der elektronische Austausch über eine gesicherte Verbindung (Web-Portal des Verantwortlichen mit Zugangsbeschränkungen) oder die klassische postalische Zusendung.
Da bei der betreffenden Kreisverwaltung keine den vorgenannten Anforderungen entsprechende Infrastruktur existierte, haben wir die Empfehlung ausgesprochen, für die E-Mail-Kommunikation eine datenschutzgerechte Lösung zu schaffen. Dieses könnte beispielsweise durch die Einrichtung eines Web-Portals, die Bereitstellung verschlüsselter Kontaktformulare oder einer Ende-zu-Ende-Verschlüsselung erfolgen.
Dieser Empfehlung ist die Verwaltung gefolgt und setzt aktuell entsprechende Maßnahmen um.
Weitere Hinweise zu diesem Thema sind in der vom Arbeitskreis Technische und organisatorische Datenschutzfragen herausgegebenen Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ zusammengestellt[38].

[38] https://www.datenschutz-mv.de/datenschutz/publikationen/broschueren/

8.3 Videoüberwachung

8.3.1 Beschwerden zur Videoüberwachung

Auch im Jahr 2020 musste sich der Landesbeauftragte für Datenschutz und Informationsfreiheit mit zahlreichen Beschwerden zur Videoüberwachung befassen. Einen besonders hohen Anteil hatten dabei Beschwerden zu Videoüberwachungsanlagen in der Nachbarschaft. Für die Betroffenen ist es oft nicht ohne Weiteres ersichtlich, welche Bereiche durch eine Kamera erfasst werden. Dadurch fühlen sich die Betroffenen oftmals durch das Vorhandensein einer Videokamera in der Nähe ihres privaten Umfeldes gestört. Häufig ist dabei die Beobachtung des Nachbargrundstückes oder des öffentlichen Bereiches durch den Verantwortlichen überhaupt nicht gewollt, da dieser lediglich sein eigenes Grundstück mit einem Überwachungssystem schützen möchte.
Sofern die Videoüberwachung nicht lediglich für private Filmaufnahmen dient, die für persönliche oder familiäre Zwecke angefertigt werden, ist die Europäische Datenschutz-Grundverordnung (DS-GVO) grundsätzlich anwendbar. So sollten sich die Betreiber von Videoüberwachungsanlagen schon vor der Installation mit der geltenden Rechtslage auseinandersetzen und prüfen, ob die geplante Videoüberwachungsanlage auch den Anforderungen der DS-GVO entspricht.
Eine wichtige Hilfe dabei ist die von der Datenschutz-Konferenz herausgegebene Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“. Diese wurde zum September 2020 grundlegend überarbeitet und an die rechtlichen Rahmenbedingungen der seit dem 25. Mai 2018 geltenden Datenschutz-Grundverordnung angepasst. Dabei wurden die Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte (Version 2.0, angenommen am 29. Januar 2020) berücksichtigt. Mit der Orientierungshilfe erhalten Betroffene und Verantwortliche Informationen über die Voraussetzungen für eine datenschutzgerechte Videoüberwachung in unterschiedlichen Lebensbereichen. In deren Anhang finden sich Muster für Hinweisschilder, die es den Verantwortlichen erleichtern, den Transparenzpflichten gemäß Art. 12 ff. DS-GVO nachzukommen. Darüber hinaus wird eine Checkliste mit den wichtigsten Prüfungspunkten im Vorfeld einer Videoüberwachung bereitgestellt.
Bei einer Beschwerde musste sich der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern mit Kameras vor zwei benachbarten Garagen in einem Wohngebiet beschäftigen.
Zur Sachverhaltsaufklärung wurden die Verantwortlichen angewiesen, Informationen zur installierten Videoüberwachung bereitzustellen. Die Verantwortlichen gaben an, ihre Fahrzeuge vor der gepachteten Garage und die Garagentore vor Vandalismus schützen zu wollen. Konkrete Vorfälle aus der Vergangenheit konnten auch auf Nachfrage hin nicht benannt werden.
Gemäß Art. 6 Abs. 1 lit. f DS-GVO ist die Videoüberwachung als Datenverarbeitung dann zulässig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die entgegenstehenden Interessen der betroffenen Personen oder Grundrechte und Grundfreiheiten dem nicht überwiegen. Berechtigte Interessen des Verantwortlichen umfassen alle rechtlichen, wirtschaftlichen, tatsächlichen oder ideellen Interessen.
Eine Videoüberwachung der von den Verantwortlichen gepachteten Garagen, die auch nur von ihnen alleine genutzt werden, ist grundsätzlich zulässig. Diese Maßnahme ist von der Wahrnehmung des Hausrechts gedeckt, welches als ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 lit. f DS-GVO anzusehen ist. Die Beobachtungsbefugnis des Hausrechtsinhabers endet jedoch grundsätzlich an den Grundstücksgrenzen. Die Grundstücksgrenze ist in diesen Fällen die Außenmauer der Garage.

Ein konkretes Überwachungsinteresse rechtfertigt regelmäßig keine Videoüberwachung öffentlich zugänglicher Räume wie Straßen, Gehwege oder Parkplätze. Nachbarn, Passanten, Kinder, Lieferanten, Besucher und sonstige Verkehrsteilnehmer müssen eine dauerhafte und gegebenenfalls anlasslose Überwachung in Wohngebieten nicht hinnehmen. In diesen Bereichen überwiegen grundsätzlich die schutzwürdigen Interessen der Betroffenen. Eine Rundumüberwachung des sozialen Lebens kann auch anhand zivilrechtlicher Maßstäbe nicht mit dem Schutz vor Schmierereien, Verschmutzungen oder einmaligem Vandalismus gerechtfertigt werden. Regelmäßig überwiegen hier die schutzwürdigen Interessen der betroffenen Bewohner und deren Besucher.
Die Verantwortlichen wurden nach § 28 VwVfG M-V vor Erlass einer Maßnahme (z. B. Verwarnung und Anweisung, die Kameratechnik zu entfernen) nach Art. 58 Abs. 2 lit. b und c DS-GVO angehört. Das haben im vorliegenden Fall die Verantwortlichen zum Anlass genommen und die Kameratechnik unverzüglich zurückgebaut. Für die bisherige Überwachung mit den Kameras wurden den Verantwortlichen Verwarnungen gemäß Art. 58 Abs. 2 lit. b DS-GVO ausgesprochen. Bußgelder wurden hier nicht verhängt.
In anderen Fällen wurden Beschwerden vorgelegt, bei denen sich eine Videoüberwachung als Überwachung mit Kameraattrappen entpuppte. Die DS-GVO findet bei der Verwendung von Kameraattrappen keine Anwendung, da keine Verarbeitung von personenbezogenen Daten stattfindet. Dies bedeutet jedoch nicht, dass Attrappen uneingeschränkt eingesetzt werden dürfen. Durch Attrappen entsteht der Eindruck einer Überwachung. Daher wird auch durch funktionslose Geräte das Persönlichkeitsrecht der betroffenen Person beeinträchtigt. Im Fall von Persönlichkeitsrechtsverletzungen können betroffene Personen zivilrechtliche Ansprüche gegen den Betreiber geltend machen. Die Maßstäbe des Datenschutzrechts sollten deshalb entsprechend angewendet werden.

8.3.2 Videogestützte Verkehrsanalyse an der Warnowquerung

Im Juli des Berichtszeitraumes wurden wir um Stellungnahme zu einer geplanten Analyse des Fahrzeugaufkommens und des Verkehrsverhaltens an der Warnowquerung gebeten. Für den Zeitraum von ein oder maximal zwei Wochen sollten zwei Videokameras je Fahrtrichtung angebracht und deren Aufnahmen ausgewertet werden. Die niedrigauflösenden Kameras sollten, feststehend am Straßenrand in einer Höhe von drei bis sechs Metern, nur für die zeitlich begrenzte Nutzung installiert werden.
Der Betreiber war der Auffassung, dass aufgrund der fest eingestellten, niedrigen Aufnahmequalität (Kameraauflösung und Datenkompression) beim vorliegenden Vorhaben nicht mehr von einer Verarbeitung von personenbezogenen Daten im Sinne der Europäischen Datenschutz-Grundverordnung (DS-GVO) ausgegangen werden kann. Da die Rohdaten der Kamera eine Punktdichte von mindestens 26 mm/Pixel aufweisen, lägen sie deutlich über einer Punktdichte von 16 mm/Pixel. Diese Punktdichte war in einem Fall in Baden-Württemberg[39] als Grenzwert definiert, um generell nicht mehr von einer Videoüberwachung mit Personenbezug zu sprechen. Der Betreiber war zudem der Meinung, dass das Zusatzwissen, das zur Herstellung eines Personenbezugs erforderlich ist, unter der Berücksichtigung eines durchschnittlichen täglichen Verkehrsaufkommens von etwa 11 000 Fahrzeugen nicht oder nur mit einem unverhältnismäßigen Aufwand erlangt werden könne.

[39] „Videoauflösung, die DIN EN 62676-4 (bzw. DIN EN 50132-7) und die Frage, ob bei einer Videoüberwachung per se personenbezogene Daten erfasst werden“, Landtag von Baden-Württemberg Drucksache 16/7777, 16. Januar 2020

Wir haben dem Betreiber mitgeteilt, dass die im beschriebenen Fall dargelegte Grenze nicht ohne Weiteres auf den hiesigen Sachverhalt übertragen werden kann. Denn im Gegensatz zum dort beschriebenen Fall wird hier nicht nur das Gesicht der Person aufgenommen, sondern auch das viel größere Fahrzeug, mit dem die Person unterwegs ist. Deshalb muss sichergestellt werden, dass neben der Person auch das Fahrzeug nicht mehr identifiziert werden kann. Bei der vorgeschlagenen Pixeldichte können Fahrzeuge mit beispielsweise einer besonders auffälligen Farbgebung, Beschriftung oder Ausstattung auch ohne unverhältnismäßigen Aufwand identifiziert werden. Wir haben dem Betreiber daher mitgeteilt, dass erst ab einer Grenze von 40 mm/Pixel (entspricht dem Detektieren gem. DIN EN 62676-4) nicht mehr von einer Videoüberwachung ohne Personenbezug ausgegangen werden kann.
Neben einigen weiteren Hinweisen haben wir dem Betreiber zudem empfohlen, den Zweck und die Durchführung des Projektes ausreichend öffentlich zu kommunizieren, damit die von der Analyse von Fahrzeugaufkommen und Verkehrsverhalten betroffenen Personen transparent über die Datenverarbeitung informiert werden.
Positiv anzumerken ist neben der Tatsache, dass der Betreiber sich proaktiv an uns gewandt hat, um eine datenschutzrechtliche Einschätzung zu erhalten, auch, dass er unseren Empfehlungen in vollem Umfang gefolgt ist, sodass wir ihm eine datenschutzkonforme Durchführung bescheinigen konnten.

8.3.3 Parkplatzüberwachung durch Parkraummanagementfirma

Verschiedene Firmen bieten Servicedienstleistungen im Parkraummanagement an. Sie kontrollieren auf den Parkplätzen ihrer Kunden die Einhaltung der Bestimmungen. Werden Verstöße auf den Parkflächen festgestellt, werden diese Verstöße sowie die jeweiligen Autokennzeichen dokumentiert. Dies erfolgt grundsätzlich auch fotografisch. Betroffene Autofahrer erhalten ein „Knöllchen“, welches am parkenden Kfz befestigt wird. Wird dieses „Knöllchen“ nicht bezahlt, werden über das Autokennzeichen bei den jeweilig zuständigen Behörden (i. d. R. Kraftfahrtbundesamt, Kfz-Zulassungsstelle) die Halterdaten abgefragt. Die Betroffenen werden dann postalisch zur Zahlung aufgefordert.
Nach einer uns vorliegenden Beschwerde sollte bei diesen „Knöllchen“ die Information zur Datenverarbeitung nach Art. 13 DS-GVO fehlen. Nach unserer Einschätzung muss die Firma nicht nach Art. 13, sondern nach Art. 14 DS-GVO den betroffenen Autofahrer informieren, da die Daten nicht direkt beim Betroffenen erhoben werden. Die Fotos vom festgestellten Parkverstoß werden in aller Regel ohne Kenntnis des Fahrers aufgenommen. Dieser bekommt dies in den meisten Fällen erst mit, wenn er das „Knöllchen“ am Auto vorfindet. Zu diesem Zeitpunkt der ersten Kontaktaufnahme ist der Betroffene über die Datenverarbeitung zu informieren.
Die Parkraummanagementfirma erklärte uns gegenüber, dass die Kunden bei Einfahrt auf den Parkplatz auf die Bewirtschaftung des Parkplatzes durch die Parkraummanagementfirma und die genannten Bedingungen hingewiesen werden. Wird gegen diese Bedingungen verstoßen, ist in aller Regel eine Vertragsstrafe fällig, die durch die Firma eingetrieben wird. Die Firma übersandte uns ein Muster eines „Knöllchens“, die verteilt werden, wenn ein Parkverstoß festgestellt wurde, und erklärte hierzu, dass sie nach ihrer Auffassung mit diesem den Informationspflichten der DS-GVO nachkomme.
Durch das „Knöllchen“ werden Betroffene informiert, dass sie einen Parkverstoß begangen haben und wie dieser erfasst, dokumentiert und fotografiert wurde. Sie werden darüber informiert, dass eine Vertragsstrafe wegen Besitzstörung nach § 858 BGB fällig wird. Die verantwortliche Firma teilt auf dem „Knöllchen“ ihre Postanschrift, Telefonnummer, Faxnummer und E-Mail-Adresse sowie die Zeiten der Erreichbarkeit mit.

Der Datenschutzbeauftragte ist unter denselben Kontaktdaten zu erreichen. Weiterhin wird auf die Datenschutzerklärung auf der Internetseite unter Angabe der URL hingewiesen. Die Datenschutzerklärung auf der Internetseite der Firma enthält dann die weiteren Informationen, die der Verantwortliche nach Art. 14 Abs. 2 DS-GVO zur Verfügung stellen muss.
Es konnte somit kein Verstoß gegen die Informationspflichten nach Art. 14 DS-GVO festgestellt werden.

8.3.4 Videoüberwachung durch jüdische Gemeinde – eine Beratung, die bewegt

Eine Videoüberwachungsanlage ist grundsätzlich datenschutzrechtlich dann zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die ebenfalls von der Videoüberwachungsanlage erfasst werden könnten, überwiegen.
In unserer täglichen Arbeit werden wir im Zusammenhang mit Videoüberwachungsanlagen häufig mit vermeintlich berechtigten Interessen konfrontiert, die einer ernsthaften Abwägung nicht ansatzweise standhalten, aus Sicht der Verantwortlichen aber eine fast flächendeckende Überwachung ihrer Grundstücke bis weit in den öffentlichen Bereich hinein rechtfertigen sollen. Nicht selten wissen die Verantwortlichen überhaupt nicht, wie ihre Videoüberwachungsanlage im Detail funktioniert und ob und wo die Daten der betroffenen Personen überall gespeichert werden. Jüngst wurde das berechtigte Interesse an der Videoüberwachung durch einen Verantwortlichen mit den menschenverachtenden Worten begründet, dass sich im Eingangsbereich einer gewerblich genutzten Immobilie ein Obdachloser „eingenistet“ hätte.
Um so beeindruckender und bewegender war für uns daher der nachfolgend geschilderte Fall:
Eine jüdische Gemeinde sowie das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) hatten den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern um Beratung bezüglich einer Videoüberwachungsanlage ersucht. Das Landeskriminalamt hatte in dem Fall eine besondere Gefährdungslage festgestellt, die unter anderem eine Videoüberwachungsanlage zum Schutz der Gemeindemitglieder und Besucher erforderlich machte.
Videoüberwachungsanlagen, die auch dann laufen, wenn Publikumsverkehr stattfindet, sind generell heikel. Gerade bei Plätzen, die der Religionsausübung dienen, können durch eine solche Videoüberwachungsanlage auch höchst sensible und besonders geschützte Daten betroffener Personen verarbeitet werden. Denn diese Videoaufzeichnungen lassen Rückschlüsse auf die Religionszugehörigkeit der betroffenen Personen zu. Gleiches gilt im Übrigen etwa auch für Arztpraxen, Apotheken oder bestimmte soziale Einrichtungen. Hier können etwa hochsensible Daten der betroffenen Personen anfallen, die Hinweise auf deren Gesundheitszustand geben könnten.
Aufgrund dieses Risikos sind an die für die Zulässigkeit der Videoüberwachungsanlage erforderliche Interessenabwägung sehr hohe Anforderungen zu stellen.
In dem vorliegenden Fall war die Interessenabwägung aber sehr einfach. Auf Grundlage der Ausführungen des Landeskriminalamtes war das überwiegende berechtigte Interesse an der Videoüberwachungsanlage leicht festzustellen. Die Mitglieder und Besucher dieser jüdischen Gemeinde in Mecklenburg-Vorpommern sind nicht nur der Gefahr von Sachbeschädigungen und volksverhetzenden Schmierereien ausgesetzt, vielmehr besteht durchaus auch eine Gefährdungslage hinsichtlich ihrer körperlichen Unversehrtheit. In dieser Situation stand für uns völlig außer Frage, dass die Videoüberwachungsanlage zulässig sein muss.

Um so bemerkenswerter war das proaktive Bemühen der Verantwortlichen der jüdischen Gemeinde, deren IT-Dienstleister und der zuständigen Architektin, die Privatsphäre von Dritten, wie etwa Passanten oder Nachbarn, unbedingt zu schützen. Bereits das vorgelegte und den Anforderungen der Europäischen Datenschutz-Grundverordnung (DS-GVO) entsprechende Konzept zur Videoüberwachungsanlage war in diesem Sinne von äußerster Zurückhaltung geprägt und die Videoüberwachung auf das zwingend erforderliche Maß reduziert. Gemeinsam konnten so Einstellungen der Videoüberwachungsanlage abgestimmt werden, die das Schutzbedürfnis der jüdischen Gemeinde mit den Datenschutzinteressen der Gemeindemitglieder, der Besucher und von Dritten in Einklang bringen.
Die Professionalität und vor allem auch die außergewöhnliche Sensibilität im Umgang mit den Freiheitsrechten anderer Personen bei den Verantwortlichen der jüdischen Gemeinde, aber auch der traurige Umstand, dass überhaupt eine Videoüberwachungsanlage zum Schutz einer jüdischer Gemeinde erforderlich ist, hat uns sehr beeindruckt und bewegt.

8.4 Polizei

8.4.1 Bußgeldverfahren gegen Polizeibeamtinnen und Polizeibeamte und Verwarnung gegen das Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern (LPBK M-V)

Wir führen seit Inkrafttreten der Europäischen Datenschutz-Grundverordnung (DS-GVO) Bußgeldverfahren gegen Polizeibeamtinnen und Polizeibeamte bei Datenschutzverstößen: Insgesamt haben wir bislang 35 solcher Verfahren eingeleitet. Dabei handelt es sich ganz überwiegend um unberechtigte Abfragen in den EDV-Systemen der Polizei zu persönlichen Zwecken.
Die Verhängung eines Bußgeldes setzt immer voraus, dass der unberechtigte Zugriff auf die Datensysteme der Polizei von uns ganz konkret belegt werden kann. Grundsätzlich protokolliert die Polizei sämtliche Zugriffe auf ihre Datensysteme, daher findet sich in diesen Protokolldaten auch der für das Bußgeldverfahren erforderliche Nachweis des unberechtigten Zugriffs. Diese Protokolldaten der Polizei werden vom LPBK M-V verwaltet.
Die DS-GVO sieht vor, dass der für die Datenverarbeitung Verantwortliche auf der Grundlage von Art. 58 Abs. 1 lit a DS-GVO angewiesen werden kann, uns alle Informationen bereitzustellen, die wir für die Verfolgung des Datenschutzverstoßes benötigen. Das führt in den Bußgeldverfahren auch dazu, dass wir das LPBK M-V anweisen, uns Kopien der benötigten Protokolldaten breitzustellen.
Weil das LPBK M-V einer solchen Anweisung in einem Fall nicht gefolgt ist, sahen wir uns veranlasst, gegen das LPBK M-V eine Verwarnung nach Art. 58 Abs. 2 lit b DS-GVO auszusprechen.
Dieser Verwarnung lag folgender Sachverhalt zugrunde:
In einem Strafverfahren hatte eine KPI eine mit unserer Anfrage identische Anfrage an das LPBK M-V zu Protokolldaten gestellt. Die Anfrage der KPI wurde vom LPBK M-V am 15. Mai 2020 bearbeitet, und das Ergebnis der Prüfung wurde der KPI am selben Tag per E-Mail übermittelt, indem eine Liste mit Zugriffen der angefragten Person übersandt wurde und der fragliche Zugriff gelb herausgestellt war.
Die Bearbeitung unserer Anfrage an das LPBK M-V zu denselben Protokolldaten erfolgte am 25.0 Mai 2020. Als Ergebnis teilte uns das LPBK M-V am 5. Juni 2020 mit, es seien keine Protokolldaten zu durchgeführten Abfragen zu der von uns nachgefragten Person festgestellt worden.

Als Verantwortlicher für die Datenverarbeitung war das LBPK M-V gem. Art. 58 Abs. 1 lit a DS-GVO i. V. m. § 20 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) verpflichtet, uns alle Informationen bereitzustellen, die zur Erfüllung unserer Aufgaben erforderlich sind. Dieser Verpflichtung ist das LPBK M-V nicht nachgekommen, obwohl es möglich war, denn das LPBK M-V hatte ja dieselbe Anfrage der KPI anders beantwortet und der KPI eine Liste übersandt, auf der der fragliche Zugriff markiert war.
Daher haben wir eine Verwarnung wegen eines Verstoßes gegen Art. 58 Abs. 1 lit a DS-GVO i. V. m. § 20 Abs. 1 DSG M-V ausgesprochen.
Außerdem haben wir uns in diesem Zusammenhang den Vorgang im Rahmen einer Kontrolle beim LPBK M-V angesehen. Im konkreten Fall konnten wir im LPBK M-V aber keine Feststellungen treffen, weil in den abgefragten Datenbanken keine Daten zu dem von uns untersuchten Fall mehr vorhanden waren, obwohl dies nach den Speicherfristen des Sicherheits- und Ordnungsgesetzes Mecklenburg-Vorpommern (SOG M-V) so zu erwarten gewesen wäre. Im Nachgang der Vor-Ort-Kontrolle stellte sich heraus, dass bestimmte Protokolldaten vom LPBK M-V in eine andere Datenbank ausgelagert worden waren. Dies betraf auch die Daten des Falls, den wir untersuchen wollten. Während der Kontrolle wurde diese weitere Datenbank aber weder erwähnt noch abgefragt, weil die bei der Kontrolle anwesenden LPBK-Bediensteten offensichtlich keine Kenntnis von der Auslagerung hatten.
Verfahrensbegleitend gab es mehrere Gespräche mit dem LPBK M-V und dem Ministerium für Inneres und Europa Mecklenburg-Vorpommern. Für die Zukunft wurde vom LPBK M-V zugesagt, die Zusammenarbeit zu verbessern.
Gegen diese Verwarnung hatte das LPBK M-V zunächst Klage vor dem Verwaltungsgericht Schwerin erhoben, diese dann aber wieder zurück genommen. Für die Zukunft hat das LPBK-MV eine verbesserte Zusammenarbeit zugesagt.

Wir empfehlen der Landesregierung, uns bei der Erfüllung unseres gesetzlichen Auftrages wie erforderlich zu unterstützen.

8.5 Schule

8.5.1 Projekt Integriertes Schulmanagement-System (ISY)

Im vergangenen Berichtszeitraum haben wir bereits über das Projekt „Integriertes Schulmanagement-System“ (Projekt ISY) berichtet, siehe Fünfzehnter Tätigkeitsbericht Punkt 8.7.1. Das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern hat die Federführung für dieses Projekt. Bereits im Fünfzehnten Tätigkeitsbericht haben wir die Wichtigkeit des regelmäßigen Austausches zwischen dem Ministerium und unserer Behörde betont. Für den aktuellen Berichtszeitraum konnte unsere Empfehlung hinsichtlich des regelmäßigen Austausches umgesetzt werden. Wir beraten nun das Ministerium regelmäßig im Rahmen des ISY-Projektes zu Grundsatzfragen des Grundrechtes auf Datenschutz.
Die beginnende Corona-Pandemie im 1. Quartal 2020 sorgte auch im ISY-Projekt für Unregelmäßigkeiten. Planungshorizonte konnten nicht mehr gehalten werden und es galt, eine E-Learning-Plattform für die Schulen in Mecklenburg-Vorpommern nun schnellstmöglich bereitzustellen. Dies stellte alle Beteiligten vor große Herausforderungen. Denn der erforderliche rechtliche Rahmen zur Verarbeitung personenbezogener Daten der Schülerinnen und Schüler sowie der Lehrkräfte im Bereich des E-Learning war bisher noch nicht gesetzlich normiert.

Nach zahlreichen Gesprächen und Abstimmungsrunden zwischen dem Ministerium und unserer Behörde wurde im April 2020 eine neue Schuldatenschutzverordnung M-V SchulDSVO M-V auf den Weg gebracht. Dort findet sich nun in § 5a in Verbindung mit dem Schulgesetz M-V (SchulG M-V) die Rechtsgrundlage zur Verarbeitung personenbezogener Daten bei der Bereitstellung digitaler Lehr- und Lerninhalte. Diese Anpassung war notwendig, um den Schulen Rechtsicherheit für die Verarbeitung personenbezogener Daten im Bereich des E-Learning zu geben.
Eine weitere Herausforderung im Zusammenhang mit dem ISY-Projekt stellten die datenschutzrechtlichen Beratungen für die Bereitstellung eines zentralen Identitäten-Management-Systems (IDM) im Schulbereich dar. Die rechtliche Normierung des IDM findet sich in § 5a der neuen Schuldatenschutzverordnung M-V. Das IDM soll personenbezogene Daten für digitale Schuldienste, Lehr- und Lerninhalte bereitstellen und eine automatisierte Verwaltung der Benutzer, der Kennungen und benutzerbezogenen Berechtigungen ermöglichen. Die Nutzung des IDM ist gemäß der neuen Schuldatenschutzverordnung M-V verpflichtend, wenn eine Schule eine neue Software einführt, welche zur Erfüllung des Unterrichts- und Erziehungsauftrages, der Schulplanung, der Schulorganisation sowie der Schulaufsicht erforderlich ist. Aus datenschutzrechtlicher Sicht verantwortlich für die Einrichtung und den Betrieb des IDM ist das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern. Die Nutzung des IDM erfolgt in gemeinsamer Verantwortung der Schulen und der Schulbehörden. Die Details dazu sind in Vereinbarungen gemäß Art. 26 DS-GVO festzulegen, die zwischen Schulen und Schulbehörden abgeschlossen werden müssen.

Wir empfehlen dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, den Austausch mit unserer Behörde zum ISY-Projekt weiter fortzuführen. Zudem empfehlen wir dem Ministerium, uns im Sinne vertrauensvoller Zusammenarbeit auch künftig frühzeitig in neue Projekte mit Bezug zu datenschutzrechtlichen Grundsatzfragen einzubinden.

8.6 Soziales

8.6.1 Kein Kita-Essen ohne Schufa-Auskunft?

Im August des Berichtszeitraumes war der Presse zu entnehmen, dass vom Deutschen Roten Kreuz der Hansestadt Rostock bestätigt wurde, dass bei der Auskunftei Schufa für alle Eltern, die das Essen ihrer Kinder in den Kindertagesstätten selber zahlen müssen, eine Kreditauskunft eingeholt werde.
Da das Einholen von Bonitätsauskünften über die Eltern bei der Auskunftei Schufa in Zusammenhang mit der Aufnahme ihrer Kinder in eine Kindertageseinrichtung eine Datenverarbeitung gemäß Art. 6 Abs. 1 DS-GVO darstellt, haben wir ein Verwaltungsverfahren eingeleitet.
Ausgangspunkt ist in diesem Zusammenhang Art. 6 DS-GVO, nach dem eine Verarbeitung personenbezogener Daten dann rechtmäßig ist, wenn mindestens eine der in Absatz 1 genannten Bedingungen erfüllt ist.
Im vorliegenden Fall wird vom Kita-Betreiber darauf abgestellt, dass die Betroffenen gemäß Art. 6 Abs. 1 lit. a DS-GVO in die Schufa-Abfrage eingewilligt haben. Hier stellt sich die Frage nach der Wirksamkeit der eingeholten Einwilligung. Eine datenschutzrechtlich zulässige Einwilligung hat den Anforderungen von Art. 7 DS-GVO zu entsprechen und muss insbesondere informiert und freiwillig sein.

Zum einen müssen der betroffenen Person alle für die Einwilligung relevanten Umstände bekannt sein. Das gilt vor allem für die Rechte der betroffenen Person. Zum anderen darf die Einwilligung nicht zur Bedingung für die Vergabe der Kita-Plätze gemacht werden. Zudem ist zu beachten, dass eine unwirksame Einwilligung nicht einfach durch ein berechtigtes Interesse gemäß Art. 6 Abs. 1 lit. f DS-GVO ersetzt werden darf.
Im Falle einer Datenverarbeitung auf der Grundlage von berechtigten Interessen müssen diese der betroffenen Person transparent gemacht werden. Ebenso muss diese Person über das Widerspruchsrecht belehrt werden. Wir haben zum Erlass einer Maßnahme nach Art. 58 Abs. 2 DS-GVO eine Anhörung durchgeführt. Das Verwaltungsverfahren hierzu läuft noch.

8.7 Rechtswesen

8.7.1 AfD-Informationsportal „Neutrale Schule“ bleibt verboten

Ab dem 28. August 2019 betrieb der Landesverband Mecklenburg-Vorpommern der Partei „Alternative für Deutschland“ (AfD, Verantwortlicher) auf seiner Homepage das sogenannte Informationsportal „Neutrale Schule“. Über das Portal wurden insbesondere Schülerinnen und Schüler sowie Eltern dazu aufgefordert, Lehrerinnen und Lehrer der AfD zu melden, die sich kritisch im Schulunterricht über die AfD geäußert haben. Die AfD war der Auffassung, mit dem Portal ein vermeintliches Neutralitätsgebot an Schulen überwachen zu müssen. Dieser Auffassung trat, wie bereits der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern im Verbotsverfahren, auch das Verwaltungsgericht Schwerin entschieden entgegen. Lehrerinnen und Lehrer haben einen Bildungs- und Erziehungsauftrag, der sie verpflichtet, eine sachbezogene Auseinandersetzung mit der behandelten Problematik zu gewährleisten und Schülerinnen und Schüler zur selbstständigen politischen Meinungsbildung zu befähigen.
Das Datenschutzrecht leistet hier einen wesentlichen Beitrag. Politische Meinungen stehen als besondere Kategorien personenbezogener Daten unter besonderem Schutz der Europäischen Datenschutz-Grundverordnung (DS-GVO). Nach Art. 9 Abs. 1 DS-GVO ist die Verarbeitung von Daten, aus denen die politische Meinung der betroffenen Person hervorgeht, grundsätzlich untersagt. Nur in streng geregelten Ausnahmen ist die Verarbeitung solcher Daten zulässig. Nach der rechtlichen Bewertung des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern lag eine solche Ausnahme aber nicht vor. Als einzig mögliche Maßnahme, um einen datenschutzkonformen Zustand wieder herzustellen, wurde daher im September 2019 die Datenerhebung über das Portal untersagt und die sofortige Vollziehung dieses Verbots unter Androhung eines Zwangsgeldes angeordnet. Der Landesverband der AfD ist dem Verbot zunächst nachgekommen, erhob aber Anfechtungsklage und ist auch im einstweiligen Rechtsschutzverfahren gegen die Anordnung der sofortigen Vollziehung vorgegangen. Während bereits der Antrag der AfD auf Wiederherstellung der aufschiebenden Wirkung der Anfechtungsklage in zwei Instanzen – sowohl vor dem Verwaltungs- als auch dem Oberverwaltungsgericht - erfolglos blieb, erging am 26. November 2020 das Urteil im Hauptsacheverfahren: Danach wird die Klage des Landesverbandes der AfD abgewiesen und die Rechtmäßigkeit des Verbots bestätigt.
Neben dem deutlichen Plädoyer des Gerichts für politischen Meinungsaustausch an Schulen ist die Entscheidung auch datenschutzrechtlich wegweisend. So hat das Gericht der Auffassung der AfD eine Absage erteilt, dass Lehrerinnen und Lehrer an öffentlichen Schulen als Träger hoheitlicher Gewalt grundsätzlich nicht dem Schutzbereich des Art. 9 Abs. 1 DS-GVO unterfallen würden.

Dem war entschieden entgegenzuhalten, dass der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht ist, auf das sich jede natürliche Person berufen kann. Erfreulich ist weiterhin insbesondere die Klarstellung, dass die rein präventive Speicherung sensibler Daten allein zur Geltendmachung oder Abwehr möglicher zukünftiger Ansprüche gegen die DS-GVO verstößt und nicht mit Art. 9 Abs. 2 lit. f DS-GVO gerechtfertigt werden kann.

8.8 Datenverarbeitung durch Privatpersonen

8.8.1 Intime Fotos beim Ex-Partner

Immer wieder kommt es vor, dass sich Frauen beim Landesbeauftragten für Datenschutz melden und darüber beschweren, dass der Ex-Partner zumeist intime Fotos von ihnen nicht löscht. Im letzten Fall hatte die Beschwerdeführerin die Fotos, auf welchen sie, nach ihrer Aussage, leicht bekleidet posierte, dem ehemaligen Partner während ihrer Beziehung übersandt. Diese Beziehung endete allerdings vor mehr als drei Jahren. Aus diesem Grund hatte sie den Ex-Partner mehrfach aufgefordert, die Fotos zu löschen. Dieser Aufforderung kam er nicht nach und erklärte zuletzt gegenüber seiner Ex-Partnerin und Beschwerdeführerin, dass die Fotos verschlüsselt und sicher verwahrt werden und nur für ihn persönlich zugänglich sind. Die Fotos dienen ihm als persönliche Erinnerung.
Wir mussten der Beschwerdeführerin mitteilen, dass wir die Löschung der Fotos im Rahmen der Europäischen Datenschutz-Grundverordnung (DS-GVO) nicht anordnen können, da die Verordnung im privaten und familiären Bereich keine Anwendung findet. Die Fotos wurden im rein privaten Kontext aufgenommen und übermittelt. Erst wenn die Bilder diesen privaten Kontext verlassen würden, das heißt der Ex-Partner die Fotos veröffentlichen oder einem Dritten zugänglich machen würde, wäre die Anwendung der DS-GVO eröffnet.
Wir haben den Ex-Partner im vorliegenden Fall daher davor gewarnt, die Bilder so zu verwenden, dass der private Bereich verlassen wird. Wir haben ferner mitgeteilt, dass im Falle des Verlassens des privaten Bereiches durch zum Beispiel eine Veröffentlichung oder Offenbarung der Bilder gegenüber Dritten, durch uns die Einleitung eines Ordnungswidrigkeitenverfahrens geprüft werden würde.
Weiterhin besteht die Möglichkeit für betroffene Frauen, ihre Forderung zivilrechtlich durchzusetzen. So hat der Bundesgerichtshof (BGH) in seinem Urteil vom 13. Oktober 2015 - VI ZR 271/14 erklärt, dass der Abgebildeten gegen den Ex-Partner nach dem Ende der Beziehung ein Löschanspruch wegen der Verletzung ihres Persönlichkeitsrechts zustehen kann. Eine Verletzung des Persönlichkeitsrechts kann bei solchen Fotos grundsätzlich vorliegen, weil der Ex-Partner eine gewisse Herrschafts- und Manipulationsmacht über die Abgebildete erlangt, selbst wenn eine Verbreitung oder Weitergabe an Dritte nicht beabsichtigt ist. Diese Macht ist um so größer, je intimer die Fotos sind.

9 Abkürzungsverzeichnis

AfD	Alternative für Deutschland
AGB	Allgemeine Geschäftsbedingungen
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
AO	Abgabenordnung
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BiKo M-V	Bildungskonzeption der 0- bis 10-Jährigen in Mecklenburg-Vorpommern
BMI	Bundesministerium des Innern, für Bau und Heimat
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CIA	Central Intelligence Agency
CSG	ComputerSpielSchule Greifswald
DAkkS	Deutsche Akkreditierungsstelle
DES	Data Encryption Standard
DIN	Deutsches Institut für Normung e. V.
DPA	Data Protection Addendum
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DS-GVO	Europäische Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EDV	elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
eGo-MV	Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern
EGovG M-V	E-Government-Gesetz Mecklenburg-Vorpommern
E.O.	Executive Order
EU	Europäische Union
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FITKO	Föderale IT-Kooperation
GG	Grundgesetz
GnuPG	GNU Privacy Guard
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
ID	Identifikationsnummer
IDM	Identitäten-Management-System
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
ISY	Integriertes-Schulmanagement-System

Kfz	Kraftfahrzeug
KiföG M-V	Kindertagesförderungsgesetz Mecklenburg-Vormpommern
KoSIT	Koordinierungsstelle für IT Standards
KPI	Kriminalpolizeiinspektion
LAKOST MV	Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern
LJR M-V	Landesjugendring Mecklenburg-Vorpommern
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LPBK MV	Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern
LT-Drs.	Landtags-Drucksache
MMV	Medienanstalt Mecklenburg-Vorpommern
mpfs	Medienpädagogischer Forschungsverbund Südwest
NSA	National Security Agency
noyb	My Privacy is None of your Business
OpenPGP	Open Pretty Good Privacy
OSTs	Online Services Terms
OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Onlinezugangsgesetz
PDF	Portable Document Format - plattformunabhängiges Dateiformat für Dokumente
RegMoG	Registermodernisierungsgesetz
SARS-CoV-2	Severe acute respiratory syndrome coronavirus type 2
SchulDSVO M-V	Schuldatenschutzverordnung Mecklenburg-Vorpommern
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
SSL	Secure Sockets Layer
SMTP	Simple Mail Transfer Protocol
S/MIME	Secure / Multipurpose Internet Mail Extensions
Steuer-ID	Steueridentifikationsnummer
StPO	Strafprozessordnung
TEO	Tage ethischer Orientierung
TLS	Transport Layer Security
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.
TR	Technische Richtlinie
USA	Vereinigte Staaten von Amerika
vdek e. V.	Verband der Ersatzkassen e. V.
VPN	Virtual Private Network
VwVfG M-V	Landesverwaltungsverfahrensgesetz
WWW	World Wide Web