2. Tätigkeitsbericht

des

Medienbeauftragten für den Datenschutz

bei der Bayerischen Landeszentrale für neue Medien

(Berichtszeitraum ist das Kalenderjahr 2020)

Herausgeber:
Der Medienbeauftragte für Datenschutz
bei der Bayerischen Landeszentrale für neue Medien
Heinrich-Lübke-Straße 27
81737 München
datenschutzaufsicht@blm.de
https://mediendatenbeauftragter.blm.de

Vorbemerkung

Anders als in den meisten anderen Bundesländern liegt die Datenschutzaufsicht im Freistaat Bayern in mehreren Händen: Neben dem *Bayerischen Landesbeauftragten für den Datenschutz* und dem *Bayerischen Landesamt für Datenschutzaufsicht* ist der *Medienbeauftragte für den Datenschutz* die zuständige Aufsicht über die privaten Rundfunkanbieter in Bayern, die *Bayerische Landeszentrale für neue Medien* und die mit ihr verbundenen Unternehmen. Daneben bestehen eine eigenständige Datenschutzaufsicht über den Bayerischen Rundfunk durch den *Rundfunkdatenschutzbeauftragten* beim *Bayerischen Rundfunk* in Umsetzung der rundfunkrechtlichen Staatsfernevorgaben des Grundgesetzes und Aufsichtsinstitutionen der Kirchen im Rahmen ihres Selbstverwaltungsrechtes nach Artikel 140 Grundgesetz.

Mit dem Übergang zur Datenschutzgrundverordnung (DS-GVO) am 25. Mai 2018 wurde durch den Bayerischen Gesetzgeber mit dem Medienbeauftragten für den Datenschutz eine eigene Aufsichtsbehörde im Sinn des Art. 51 DS-GVO für das bayerische private Rundfunkmodell geschaffen. Aufbauend auf den vormaligen Beauftragten für den Datenschutz bei der Landeszentrale wurde mit zwei neuen Referentenstellen in 2018, einer halben Assistentenstelle in 2019 und einer weiteren halben Referentenstelle in 2020 die Aufsichtsinstitution weiter aufgebaut.

Dieser Bericht gibt zunächst einen Überblick über Positionierung, Aufgaben und Tätigkeitsbereiche des Medienbeauftragten, sowie die Zusammenarbeit mit anderen Aufsichtsbehörden bevor ein Blick auf die aktuelle gesetzliche Entwicklung in Datenschutzfragen für den Medienbereich geworfen wird: Hier sind vor allem das Urteil des Europäischen Gerichtshofs (EuGH) zum internationale Datenverkehr auf der Grundlage des EU-US Privacy-Shield (Schrems II) sowie die Umsetzungsentscheidung des BGH in Sachen *Planet 49* zu nennen, in welchem aufbauend auf eine Entscheidung des EuGH aus 2019 der BGH insbesondere über die Frage der weiteren Anwendbarkeit des Telemediengesetztes entschied. Beide Urteile betreffen zahlreiche Rundfunkanbieter in zentralen Punkten.

Im Anschluss erläutern wir unsere Aktivitäten anhand von Fallbeispielen: Neben Anfragen zum Thema *One Stop Shop*, zur Gestaltung von Datenschutzerklärungen, zur Reichweitenmessung, zu Löschkonzepten und zum Medienprivileg beschäftigten uns zahlreiche Beschwerden und Kontrollanregungen, wie beispielsweise zu den Themen Altersprüfung, Cookiebanner, *Consent*- und *Tracking Tools sowie Datentransfers in Drittstaaten*. Schließlich nahmen die Meldungen der Verletzung des Schutzes personenbezogener Daten (sogenannte Datenpannen) häufig aufgrund von Fehlversendungen wie auch in Verbindung mit Aktivitäten der Cyberkriminalität, und verlorene Datenträger einen großen Teil unserer Aufsichtstätigkeiten ein. Einige relevante Zah-

len und Fakten zu unseren Tätigkeiten liefern einen abschließenden Überblick und leiten zum Ausblick ins neue Jahr 2021 über.

Der vorliegende Bericht über das Kalenderjahr 2020 soll einen Einblick in unsere Aufgaben und Tätigkeitsfelder liefern und gleichsam auch die Schwerpunkte unserer Arbeit in dieser Berichtsperiode herausstellen. Er ist der zweite des Medienbeauftragten für den Datenschutz, der nach Geltung der Datenschutz-Grundverordnung erstellt wird.

München, 19.06.2021

Andreas Gummer
Medienbeauftragter für den Datenschutz
Bayerische Landeszentrale für neue Medien (BLM)

Inhalt

1. Der Medienbeauftragte für den Datenschutz und seine Aufgaben

1.1 Rechtliche Einordnung als Aufsicht

Der Medienbeauftragte für den Datenschutz (Mediendatenbeauftragter) ist nach Art. 20 Abs. 1 des Gesetzes über die Entwicklung, Förderung und Veranstaltung privater Rundfunkangebote und anderer Telemedien in Bayern (Bayerisches Mediengesetz – BayMG) die zuständige Aufsichtsbehörde im Sinne des Art. 51 der Verordnung (EU) 2016/679 Datenschutz-Grundverordnung (DS-GVO) für

- die Bayerische Landeszentrale für neue Medien (BLM),
- die Unternehmen, an denen die Landeszentrale zu mindestens 50 Prozent beteiligt ist und deren Geschäftszweck im Aufgabenbereich der Landeszentrale nach Art. 11 BayMG liegt, und
- die Anbieter[1].

Der Mediendatenbeauftragte überwacht bei diesen Stellen die Einhaltung der Vorgaben des Datenschutzrechts. Sein sektorspezifischer Zuständigkeits- und Aufsichtsbereich ist dort aber nicht auf die Überwachung der Einhaltung der speziell für den Medienbereich geltenden – oder besser: die meisten Regelungen der DS-GVO ersetzenden – Datenschutzvorschriften beschränkt (zu nennen sind hierbei insbesondere die Vorgaben zum sogenannten *Medienprivileg* des Art. 85 DS-GVO, vgl. 3.1.4). Im Gegenteil: Er ist bei den oben genannten Stellen sowie ggf. im Rahmen des sogenannten *One-Stop-Shop* unter bestimmten Voraussetzungen auch bei Tochterunternehmen von Anbietern (vgl. 3.1.1) umfassend für die Überwachung jeglicher datenschutzrechtlich relevanter Vorgänge zuständig.

Der Medienbeauftragte für den Datenschutz ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er unterliegt keiner Rechts- oder Fachaufsicht. Näheres zu seiner Stellung ist den Absätzen 1 bis 10 des Art. 20 BayMG sowie der von der BLM erlassenen „Satzung über den Medienbeauftragten für den Datenschutz nach dem Bayerischen Mediengesetz“ vom 23. November 2018 (AMBl 2018, S. 20) zu entnehmen.

1 Überall dort, wo es möglich ist, werden in diesem Bericht geschlechtsneutrale Formulierungen verwendet. Ansonsten wird auf das generische Maskulinum zurückgegriffen. Dort, wo es bedeutungstragend ist, werden die jeweiligen geschlechtsspezifischen Formen angewandt.

1.2 Aufgaben und Befugnisse

Die Aufgaben und Befugnisse des Mediendatenbeauftragten ergeben sich insbesondere aus Art. 57, 58 Abs. 1-5 DS-GVO. Er verfügt somit über einen umfangreichen Katalog an Befugnissen, die von den Untersuchungsbefugnissen des Art. 58 Abs. 1 DS-GVO über konkrete Abhilfebefugnisse des Art. 58 Abs. 2 DS-GVO (umfassend die präventive Warnung, die repressive Verwarnung sowie konkrete Anweisungs- und Anordnungsbefugnisse) bis hin zur Sanktion der Verhängung von Geldbußen nach Art. 83 DS-GVO als „schärfstem Schwert" der nach der DS-GVO vorgesehenen Maßnahmen reichen. Eine Einschränkung besteht lediglich im Hinblick auf die BLM, der gegenüber keine Geldbußen vorgesehen sind (Art. 20 Abs. 6 Satz 3 BayMG).

1.3 Zusammenarbeit mit anderen Behörden und Institutionen

Der Medienbeauftragte für den Datenschutz wird gegenüber den Anbietern, die in der üblicherweise geltenden Terminologie zum nicht-öffentlichen Bereich zu rechnen wären, anstelle des hierfür ansonsten zuständigen *Bayerischen Landesamtes für Datenschutzaufsicht*, und gegenüber der Landeszentrale und ihren Tochterunternehmen (im Sinne des Art. 20 Abs. 1 Satz 2 lit. b BayMG) anstelle des für den öffentlichen Bereich in Bayern in der Regel zuständigen *Bayerischen Landesbeauftragten für den Datenschutz* tätig.

Darüber hinaus bestehen aus verfassungsrechtlichen Gründen für den *Bayerischen Rundfunk* und bestimmte seiner Beteiligungsunternehmen eine eigenständige Aufsichtszuständigkeit durch den Rundfunkdatenschutzbeauftragten und unter den in Art. 91 DS-GVO genannten Voraussetzungen spezifische Aufsichtsbehörden für den kirchlichen und religiösen Bereich.

Für die bayerischen Datenschutzaufsichtsbehörden sieht Art. 21 BayDSG vor, dass sie regelmäßig die in Erfüllung ihrer Aufgaben gewonnen Erfahrungen austauschen und sich gegenseitig in ihrer Aufgabenwahrnehmung unterstützen. In Erfüllung dieser Vorgabe fand insbesondere mit dem *Bayerischen Landesamt für Datenschutzaufsicht* im Berichtszeitraum ein reger Austausch zu unterschiedlichsten Aufsichtsfragen sowie wechselseitig zuständigkeitsbedingten Abgaben statt. Zuständigkeitsfragen bereiten im Rundfunkdatenschutz deshalb besondere Schwierigkeiten und waren daher immer wieder ein maßgebliches Thema, da diese im Datenschutzrecht üblicherweise nach dem Sitzlandprinzip entschieden werden, während unter der Geltung des RStV die aufsichtliche Zuständigkeit für Angebote jenseits des landesweiten Rundfunks einer Auswahlentscheidung des jeweiligen Anbieters überlassen war, der mit seiner Antragstellung bei einer Landesmedienanstalt seiner Wahl deren Zuständigkeit begründen konnte. Mit dem Übergang zum MStV hat sich der Gesetzgeber für die Zukunft nun auch beim

Rundfunk für die Anwendung des Sitzlandprinzips entschieden,[2] für bereits bestehende Zulassungen und Genehmigungen jedoch die Fortführung der alten Zuständigkeiten nach RStV angeordnet.[3] Da Aufsichtstätigkeiten gegenüber Rundfunkveranstaltern aus verfassungsrechtlichen Gründen zudem dem Staatsfernegebot unterliegen, eröffnen Überschneidungen unterschiedlicher Zuordnungskriterien immer wieder offene Fragestellungen.

Neben dem gesetzlich durch Art. 21 BayDSG vorgesehenen Erfahrungsaustausch mit den bayerischen Aufsichtsbehörden nahm der Mediendatenbeauftragte im Berichtsjahr auch an unterschiedlichen Terminen zum Erfahrungsaustausch mit anderen (Datenschutz-) Aufsichtsbehörden teil:

Bedeutsam waren vor allem die Sitzungen des Arbeitskreises Medien (AK Medien) der Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), sowie der institutionalisierte Austausch der DSK mit den spezifischen Aufsichtsbehörden,[4] der üblicherweise zweimal jährlich stattfindet.

Über diesen eher generelle Themen behandelnden institutionalisierten Austausch hinaus stimmte sich der Mediendatenbeauftragte auch in konkreten Aufsichtsfällen länder- und behördenübergreifend ab: So gab es insbesondere im Frühjahr 2020 einen intensiven Austausch mit der Behörde des Hamburger Beauftragten für Datenschutz und Informationsfreiheit sowie der Bundesnetzagentur bezüglich des aufsichtlichen Vorgehens gegen einen außerbayerischen Auftragsverarbeiter eines bayerischen Rundfunkanbieters im Bereich der illegalen Telefonwerbung.

Im Hinblick auf die europaweit eingelegten 101 Beschwerden[5] des Vereins NOYB – European Center for Digital Rights fand mit den anderen betroffenen deutschen Behörden ein regelmäßiger Austausch über das weitere Vorgehen statt. Zudem wurde beim Europäischen Datenschutzausschuss (im Folgenden: EDSA) auch eine Task Force für diese sog. 101 Beschwerden eingerichtet, um eine einheitliche Vorgehensweise und Rechtsanwendung auch auf europäischer Ebene zu gewährleisten, an der sich der Medienbeauftrage regelmäßig beteiligt (vgl. hierzu ausführlicher unter 3.2.6.).

Auch in Zusammenhang mit weiteren Verfahren steht der Mediendatenbeauftragte im Austausch mit anderen Aufsichtsbehörden. Besonders hervorzuheben ist der Austausch mit der österreichischen Datenschutzbehörde (DSB). Hier ging es schwerpunktmäßig um Fragen im

[2] Vgl. § 106 MStV
[3] Vgl. § 119 Abs. 1 S. 1 MStV
[4] Der Begriff entstammt § 18 Abs. 1 S. 4 BDSG, der damit die nach den Artikeln 85 und 91 DS-GVO eingerichteten Aufsichtsbehörden bezeichnet. Dieser Begriff ist insoweit missverständlich oder zumindest jedenfalls unscharf und letztlich zweifelhaft, als er Aufsichtsinstitutionen mit sehr verschiedenen Zuständigkeiten und Grundkonzepten gleichermaßen umfassen kann.
[5] Das Gemeinsame der Beschwerden liegt in den Datentransfers ins nichteuropäische Ausland, die durch bestimmte in die angesprochenen Datenverarbeitungsprozesse eingebundene Tools ausgelösten werden.

Zusammenhang mit Verantwortlichen aus Bayern und deren Tochterunternehmen, die in Österreich niedergelassen sind. Im Sinne einer einheitlichen Rechtsauslegung erschien bei einer möglichen grenzüberschreitenden Betroffenheit ein bilateraler Austausch sachgerecht.

Im Zusammenhang mit einer geplanten BayMG-Novelle hatte der Medienbeauftrage zudem der federführenden Bayerischen Staatskanzlei Anregungen und Änderungsvorschläge übermittelt und mit dieser erörtert, die jedoch bisher im Gesetzgebungsverfahren noch keine Berücksichtigung finden konnten.

2. Interessante Entwicklungen im Fokus

2.1 Wichtige gesetzliche Änderungen und Vorhaben

Wieder einmal zum Erliegen kamen auf EU-Ebene Ende 2020 die Verhandlungen für die umstrittene ePrivacy-Verordnung für den Datenschutz in der elektronischen Kommunikation. Nach dem Willen der EU-Kommission sollte diese ursprünglich bereits im Mai 2018 die Datenschutzrichtlinie für elektronische Kommunikation aus dem Jahr 2002 (ePrivacy-Richtlinie 2002/58/EG) ablösen und parallel mit der DS-GVO in Kraft treten. Sie sollte in Ergänzung und Überlagerung der Vorschriften der DS-GVO insbesondere Kommunikationsvorgänge und den Datenschutz im Bereich der elektronischen Kommunikation und damit auch im Bereich sozialer Netzwerke regeln. Auch unter der deutschen Ratspräsidentschaft in der zweiten Jahreshälfte 2020 konnten letztlich keine Fortschritte im Gesetzgebungsprozess erzielt werden. Zwar wurde durch die Bundesregierung bereits Anfang Juli 2020 ein Diskussionspapier zur Wiederaufnahmen der Verhandlungen veröffentlicht und im November 2020 auch ein entsprechender Textvorschlag vorgelegt. Dieser Kompromissvorschlag wurde durch die zuständige Arbeitsgruppe jedoch abgelehnt. Die deutsche Ratspräsidentschaft konnte daher in der zweiten Novemberhälfte 2020 lediglich einen Fortschrittsbericht präsentieren und gab das Thema an Portugal weiter, das ab Januar 2021 die Ratspräsidentschaft übernahm.

Dies ist weiterhin eine sehr unglückliche Situation: Fragen des Nutzer-Tracking für zielgerichtete Werbung, des Setzens von Cookies bzw. der Umgang mit bestimmten Meta-Daten bleiben so auch weiterhin ungeregelt bzw. unabgestimmt mit den insoweit lückenhaften Regelungen der DS-GVO und unterfallen weiterhin dem von vielen als „veraltet" empfundenen Regelungsrahmen der ePrivacy-Richtlinie.

Parallel zu den erfolglosen Bemühungen auf EU-Ebene kamen auf nationaler Ebene die Bemühungen um die Schaffung angepasster und einheitlicherer Datenschutzregelungen in der elektronischen Kommunikation hingegen zumindest teilweise voran: Nicht zuletzt im Zuge des Urteils des BGH vom 28.05.2020, Az. I ZR 7/16 – Cookie-Einwilligung II (vgl. hierzu näher unten 2.2.2) arbeitete das Bundesministerium für Wirtschaft und Technologie an einem „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien (Telekommunikations-Telemedien-Datenschutz-Gesetz – TTDSG), zu dem im Berichtszeitraum ein interner Referentenentwurf mit Bearbeitungsstand vom 14.07.2020 an die Öffentlichkeit gelangt ist. Demzufolge soll die Neuregelung auch dazu dienen, die Verwirklichung eines „wirksamen und handhabungsfreundlichen Datenschutzes und Schutzes der Privatsphäre zu erleichtern, insbesondere mit Blick auf die in vielen Fällen erforderliche Einwilligung in die Verarbeitung von Verkehrs- und Standortdaten oder in das Speichern und Abrufen von

Informationen auf Endeinrichtungen der Endnutzer.“ Die Datenschutz-Bestimmungen des TMG und des TKG, einschließlich der Bestimmungen zum Schutz des Fernmeldegeheimnisses, sollen aufgehoben, in einem neuen Gesetz zusammengeführt und dabei auch die Anforderungen der DS-GVO aufgenommen werden. Vor allem aber sollen die seit langem überfälligen Anforderungen der ePrivacy-Richtlinie[6] aus dem Jahr 2009 umgesetzt werden, die im Zentrum der o.g. BGH-Entscheidung[7] standen. Das Gesetzgebungsverfahren war zum Ende des Berichtszeitraums noch nicht angeschlossen. Das TTDSG wird, wenn auch in abgeänderter Form, wohl zum Ende des Jahres 2021 in Kraft treten.

Am 07.11.2020 ist der neue Medienstaatsvertrag (MStV) in Kraft getreten, der den Rundfunkstaatsvertrag ablöst. Damit gehen einige Veränderungen einher, die für den Rundfunkdatenschutz von Bedeutung sind. Zu nennen sind hierbei vor allem die Anpassungen des einfachgesetzlichen Rundfunkbegriffs,[8] die sich insbesondere aus der wieder eingefügten Erwähnung einer journalistisch-redaktionellen Gestaltung in der Begriffsdefinition des § 2 Abs. 1 S. 1 selbst, den Klarstellungen in den Begriffsbestimmungen des § 2 Abs. 2 Nr. 1-3 und den Neuerungen des § 54 ergeben. Bisher nur angezeigte Internethörfunkangebote gelten künftig als zugelassene Programme;[9] zudem treten neben den zugelassenen Rundfunk künftig auch zulassungsfreie Rundfunkprogramme.[10] Zudem wurde das Zuständigkeitsregime für neu zuzulassende Programme auf das Sitzlandprinzip umgestellt.[11] Und schließlich ist das Medienprivileg für den Rundfunk in § 12 MStV und für den Bereich der Telemedien in § 23 MStV überführt worden.[12]

[6] Datenschutzrichtlinie für elektronische Kommunikation aus dem Jahr 2002 (ePrivacy-Richtlinie 2002/58/EG)
[7] Urteils des BGH vom 28.05.2020, Az. I ZR 7/16 – Cookie-Einwilligung II (vgl. hierzu näher unten 2.2)
[8] Der deutlich weitere verfassungsrechtliche Rundfunkbegriff ist hiervon selbstverständlich nicht betroffen, so dass die Folgerungen der verfassungsrechtlich vorgegebenen Rundfunkfreiheit hier unberührt bleiben.
[9] Vgl. § 54 Abs. 2 MStV
[10] Vgl. § 54 Abs. 1 S. 1 MStV
[11] Vgl. § 106 Abs. 1 i.V.m. § 119 Abs. 1 S. 1 MStV
[12] Vgl. unten 3.1.4

2.2 Urteile zum EU-US Privacy-Shield bzw. zur weiteren Anwendung des TMG: Herausforderungen für die Aufsichtspraxis

2.2.1 internationaler Datenverkehr auf der Grundlage des EU-US Privacy-Shield („Schrems II")

Mit seinem Urteil vom 16.07.2020[13] hat sich der EuGH durch seine große Kammer zum zweiten Mal zur Frage geäußert, unter welchen Voraussetzungen ein Datentransfer aus dem europäischen Rechtsraum in die USA zulässig ist.

Den Hintergrund hierfür bilden europarechtliche Vorgaben, die bereits seit längerem für eine Übermittlung personenbezogener Daten in sogenannte Drittländer voraussetzen, dass im Zielland des Transfers ein vergleichbares Datenschutzniveau wie in Europa besteht. Das Europarecht verfolgte damit die Zielsetzung sicherzustellen, dass das durch europäisches Recht vorgegebene Schutzniveau für natürliche Personen nicht untergraben wird.[14] Die Übermittlung personenbezogener Daten in Drittländer ist daher nur zulässig, wenn die in Kap. 5 der DS-GVO niedergelegten Bedingungen eingehalten werden.

Im Hinblick auf die USA hatte bis zum Jahr 2015 eine Entscheidung der EU-Kommission vom 06.07.2000 bescheinigt, dass die seinerzeit geltenden „Safe-Harbour-Bedingungen", die ein vergleichbares Schutzniveau bildeten, in den USA unter bestimmten Voraussetzungen eingehalten würden. Diese Entscheidung der EU-Kommission hatte der EuGH in einem Urteil vom 06.10.2015[15] in einem Verfahren von Max Schrems gegen die irische Datenschutzaufsichtsbehörde (DPC) für ungültig erklärt.

Daraufhin hatte die EU-Kommission mit der US-Regierung ein EU-US Privacy Shield-Abkommen abgeschlossen, das die vormalige Safe-Harbour-Entscheidung ersetzte und ab dem 01.08.2016 die Basis für die Übermittlung personenbezogener Daten in die USA darstellte. Der das Privacy Shield betreffende Durchführungsbeschluss der EU-Kommission[16] wurde in dem oben genannten Urteil vom 16.07.2020 abermals in einem Verfahren der DPC gegen Max Schrems (in diesem Falle zusammen mit Facebook Irland) für ungültig erklärt. Maßgeblich war, dass die auf amerikanische Rechtsvorschriften gestützten Überwachungsprogramme amerikanischen Behörden das Recht geben, auf personenbezogene Daten aus der EU zuzugreifen und sie zu verwenden, so dass dies zu Einschränkungen des Schutzes führt. Insgesamt würde sich kein Schutzniveau ergeben, das dem europäischen der Sache nach gleichwertig wäre. Zudem stellte der Gerichtshof fest, dass für amerikanische Behörden zwar Anforderungen bestünden, die betroffenen Personen jedoch keine Rechte hätten, diese gegenüber amerikanischen Behörden

[13] Urteil des EuGH vom 16. Juli 2020 (Rechtssache C 311/18 – „Schrems II")
[14] Vgl. Art. 44 S. 2 DS-GVO
[15] Urteil des EuGH vom 6. Oktober 2015 (Rechtssache C-362/14 – „Schrems I")
[16] Durchführungsbeschluss (EU) 2016/1250

gerichtlich durchzusetzen. Auch der im Privacy Shield vorgesehene Ombudsmechanismus würde entgegen den Feststellungen der Kommission den betroffenen Personen keinen Rechtsweg bieten, der den nach dem EU-Recht erforderlichen Garantien der Sache nach gleichwertig wäre.

Zwar kann ein gleichwertiges Schutzniveau auch durch andere Garantien wie z.B. Standardvertragsklauseln sichergestellt werden; dies setzt jedoch voraus, dass die fraglichen Garantien eingehalten werden und auch eingehalten werden können. Insoweit hebt der EuGH hervor, dass der Datenexporteur und der Empfänger der Übermittlung vorab prüfen müssen, ob das erforderliche Schutzniveau so in dem betreffenden Drittland eingehalten wird. Gegebenenfalls muss der Empfänger dem Datenexporteur mitteilen, dass er die Standardschutzklauseln nicht einhalten kann.

Nachdem die ein angemessenes Schutzniveau in den USA feststellende Entscheidung der EU-Kommission für ungültig erklärt wurde, obliegt es dem Datenexporteur, die Sach- und Rechtslage zu überprüfen, wobei sich stets die Schwierigkeit ergeben wird, wie im Falle eines amerikanischem Recht entsprechenden Zugriffs gewährleistet werden soll, ein Schutzniveau für den betroffenen EU-Bürger sicherzustellen, welches das amerikanische Recht nicht vorsieht.

Gleichwohl hat der europäische Datenschutzausschuss am 10.11.2020 Empfehlungen beschlossen, die Maßnahmen zur Gewährleistung eines entsprechenden Schutzniveaus darstellen.

2.2.2 BGH zur Cookie- Einwilligung

Der EuGH hatte in seiner im Oktober 2019 verkündeten Entscheidung in der Rechtssache Planet 49[17] auf eine durch den Bundesgerichtshof (BGH) zur Vorabentscheidung eingereichte Vorlage hin unter anderem zur Frage Stellung genommen, welche Voraussetzungen für eine Einwilligung in Werbe- und Marketingcookies vorliegen müssen, bzw. wann eine wirksame Einwilligungserklärung angenommen werden kann.[18] Der EuGH hatte u. a. festgestellt, dass eine wirksame Einwilligung nicht vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss (sog. Opt-Out). Eine Einwilligung darf nicht vermutet werden, sondern muss sich aus einem aktiven Verhalten des Nutzers ergeben.

Auf der Grundlage der Vorgaben dieses EuGH-Urteils traf der BGH im Berichtszeitraum nun seine abschließende Entscheidung (BGH, Urteil vom 28.05.2020, Az. I ZR 7/16 – Cookie-Einwilligung II) und stellte fest, dass voreingestellte Einwilligungen (Opt-Outs) mit Blick auf Art. 5 Abs. 3 Satz 1 der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) unwirksam sind und stattdessen eine

[17] Urteil des EuGH vom 01.10.2019, C 673/17)
[18] Vgl. die ausführliche Analyse hierzu im 1. Tätigkeitsbericht des Mediendatenbeauftragten (dort unter 2.3.2.)

informierte, aktive Einwilligung im datenschutzrechtlichen Sinne erforderlich ist (Opt-In). Der BGH nahm hierbei auch zur Frage der Anwendbarkeit des § 15 Abs. 3 TMG Stellung, der seinem Wortlaut nach einem Diensteanbieter gestattet, unter anderem für Zwecke der Werbung Nutzungsprofile zu erstellen, sofern der Nutzer dem nicht widerspricht. Danach würde also eine bloße Opt-Out-Möglichkeit für den Nutzer ausreichen. Anders als die DSK in ihrer Orientierungshilfe für Anbieter von Telemedien[19] vom März 2019, die zur Frage der Einwilligung zur Verarbeitung personenbezogener Daten insgesamt von einem Anwendungsvorrang der Regelungen der DS-GVO gegenüber den Regelungen des § 15 TMG ausgeht, hält der BGH aber mit Blick auf Art. 5 Abs. 3 Satz 1 der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) eine richtlinienkonforme Auslegung des § 15 Abs. 3 TMG auch nach Inkrafttreten der DS-GVO noch für möglich und diesen damit für anwendbar. Dem stehe laut BGH auch nicht entgegen, dass der deutsche Gesetzgeber bisher keinen entsprechenden Umsetzungsakt vorgenommen habe, denn es sei anzunehmen, dass der Gesetzgeber die bestehende Rechtslage in Deutschland für richtlinienkonform erachtete und keinen Änderungsbedarf sah. Nach Ansicht des BGH kann im Fehlen einer (wirksamen) Einwilligung mit Blick darauf, dass der Gesetzgeber mit § 15 Abs. 3 S. 1 TMG das unionsrechtliche Einwilligungserfordernis umgesetzt sah, der nach dieser Vorschrift der Zulässigkeit der Erstellung von Nutzungsprofilen entgegenstehende Widerspruch gesehen werden.[20]

Der Kunstgriff des BGH, das Einwilligungserfordernis sowohl der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) als auch der DS-GVO aus der Formulierung „nicht widerspricht" in § 15 Abs. 3 Satz 1 TMG herauszulesen und das TMG so weiter für anwendbar zu halten, ist in der datenschutzrechtlichen Literatur wie auch durch Datenschutzaufsichtsbehörden stark kritisiert worden. Für die Praxis der Anbieter bedeutet das Urteil des BGH aber letztlich, dass sie den Wortlaut des § 15 Abs. 3 Satz 1 TMG ignorieren können und für den Einsatz von nicht zwingend technisch erforderlichen Cookies, insbesondere Werbe- und Marketing-Cookies, zuvor eine informierte und aktive Einwilligung des Nutzers einholen müssen (Opt-In).

Relevant ist diese Erkenntnis des BGH, weil für die Fälle, auf die das TMG anzuwenden ist, Art. 6 Abs. 1 lit. f DS-GVO wegen des TMG nicht gilt und sich somit eine Rechtsgrundlage für einen Verarbeitungsprozess nicht aus überwiegenden berechtigten Interessen des Verantwortlichen ergeben kann. Etwas Anderes kann lediglich für den Rundfunkbereich daraus abgeleitet werden, dass das TMG für den Rundfunk nie unmittelbar galt, sondern nur über § 47 Abs. 1 RStV und dann entsprechend anwendbar war. Diese Verweisung wurde durch den Rundfunkgesetzgeber aber ausdrücklich mit dem Hinweis darauf aufgehoben, dass sich datenschutzrechtliche Anforderungen künftig aus der DS-GVO unmittelbar ergeben würden. Soweit das TMG aber gar nicht mehr anwendbar ist, kann sich aus dem nicht anwendbaren TMG auch keine Umsetzung

[19] Vgl. die ausführliche Analyse hierzu im 1. Tätigkeitsbericht des Mediendatenbeauftragten, 2.4.
[20] BGH, Urteil vom 28.05.2020, Az. I ZR 7/16 – Cookie-Einwilligung II, Rz. 55.

der ePrivacy Richtlinie ergeben, die Regeln der DS-GVO wie dessen Art. 6 Abs. 1 lit. f verdrängen könnte. Für den Rundfunk lässt sich daher argumentieren, dass Art. 6 Abs. 1 lit. f DS-GVO dort nach wie vor gilt, und die Möglichkeit einer Rechtfertigung durch berechtigte Interessen des Verantwortlichen auch dort weiterhin besteht, wo außerhalb des Rundfunks das TMG als Umsetzung der ePrivacy Richtlinie die DS-GVO verdrängt.

2.3 Orientierungshilfen

Der EDSA hat im Berichtszeitraum zahlreiche Guidelines und Empfehlungen veröffentlicht. Für den Aufgabenbereich des Mediendatenbeauftragten waren insbesondere die folgenden Papiere von besonderer Relevanz:

- Guidelines 05/2020 on consent under Regulation 2016/679 vom 04.05.2020
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR vom 02.09.2020
- Guidelines 8/2020 on the targeting of social media users vom 02.09.2020
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten vom 10.11.2020)

Auch die Datenschutzkonferenz und die Europäische Kommission haben u. a. folgende wichtige Papiere veröffentlicht:

- Beschluss der DSK vom 12.05.2020 Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich
- Hinzuweisen ist auch auf die neu ausgestalteten Standardvertragsklauseln der Europäischen Kommission.[21]

[21] EU-Kommission legt Entwürfe zu neuen Standardvertragsklauseln für internationale Datentransfers vor Deutschland, https://ec.europa.eu/germany/news/20201113-datentransfers_de, Download 21.12.2020

3. Unsere Tätigkeiten

Die praktische Aufsichtstätigkeit ist zumeist geprägt durch Anfragen aus dem Kreis der Verantwortlichen, Beschwerden und Kontrollanregungen von betroffenen Bürgern und den nach Artikel 33 DS-GVO dem Mediendatenbeauftragten zu meldenden Datenpannen. Im Folgenden werden die dabei im Berichtszeitraum berührten maßgeblichen Fragenkreise dargestellt.

3.1 Anfragen

3.1.1 One-Stop-Shop bei Tochterunternehmen

Bereits in der Vergangenheit waren einige der bei der Landeszentrale zugelassenen – insbesondere bundesweiten – Rundfunk- oder Plattformanbieter derart strukturiert, dass Datenverarbeitungstätigkeiten an Tochtergesellschaften ausgelagert werden. Diese Tochtergesellschaften haben ihren Sitz auch außerhalb Bayerns. Teilweise sind sie sogar im Ausland verortet. Soweit Datenverarbeitungstätigkeiten an die Tochtergesellschaften ausgelagert werden oder dort stattfinden z.B. Kundenakquise, Nutzerverwaltung usw., und nicht ausdrücklich mittels eines Auftragsverarbeitungsverhältnisses nach Art. 28 DS-GVO zwischen Mutter- und Tochtergesellschaft geregelt sind, wirft dies die Frage nach der örtlich und sachlich zutreffenden Datenschutz-Aufsicht auf.

Da der Rundfunkdatenschutz im Grundsatz auf erteilten Rundfunkzulassungen bzw. -Genehmigungen aufbaut, spielt der Sitz eines Unternehmens insoweit bisher, anders als im allgemeinen Datenschutzrecht, das das Sitzlandprinzip generell anwendet, für die sektorspezifische Zuständigkeit des Medienbeauftragten zunächst keine bestimmende Rolle. Dennoch sind auch im Rundfunkdatenschutz die europarechtlich vorgegebenen Regeln des sogenannten One-Stop-Shop-Verfahrens zu beachten.[22] Dies gilt insbesondere für Verarbeitungsverfahren, die als grenzüberschreitend i.S.v. Art. 4 Nr. 23 DS-GVO anzusehen sind, da dann gegebenenfalls Aufsichtsbehörden andere Mitgliedstaaten der EU an den fraglichen Verfahren zu beteiligen sind.

In der konkreten Aufsichtspraxis wurden Fragestellungen zum One-Stop-Shop-Verfahren im Berichtszeitraum in mehreren Fällen behandelt. Dabei ging es darum festzustellen, wie unabhängig die jeweiligen Tochterunternehmen jeweils agieren bzw. in welchem Rahmen datenschutzrechtliche Themen zentral z.B. durch die Muttergesellschaft mit Anbieterstatus festgelegt werden. Besonderes Augenmerk verdienen in diesem Zusammenhang Veränderungen in der Konzern- bzw. Unternehmensstruktur oder Akquisitionen. Im Berichtszeitraum nicht mehr abschließend zu klären war die aufsichtliche Zuständigkeit hinsichtlich eines in Österreich

[22] Vgl. hierzu bereits ausführlich im 1. Tätigkeitsbericht des Mediendatenbeauftragten (dort 3.1.1.)

ansässigen Tochterunternehmens eines bayerischen Anbieters. In diesem Fall befindet sich der Mediendatenbeauftragte im Austausch mit der Österreichischen Datenschutzbehörde.

3.1.2 Gestaltung von Datenschutzerklärungen

Die Pflicht, eine Datenschutzerklärung mit bestimmten Informationen vorzuhalten, hat auch im Berichtszeitraum einige Verantwortliche vor Herausforderungen gestellt. Die gesetzlich festgelegten Pflichten und die dafür erforderlichen Inhalte haben zwar durch das Inkrafttreten der DS-GVO keine grundsätzlichen Änderungen erfahren. Dennoch sind sich zahlreiche Anbieter nach wie vor unsicher, was enthalten sein muss und welcher Zweck damit verfolgt wird. Der Mediendatenbeauftragte erhielt daher zum einen diverse Anfragen zur korrekten Ausgestaltung und wies zum anderen Verantwortliche auf problematische bzw. möglicherweise rechtswidrige Ausgestaltungen hin.

So waren beispielsweise in einigen Datenschutzerklärungen zwar alle erforderlichen Informationen hinterlegt, diese jedoch so unstrukturiert und unzusammenhängend dargeboten, dass es für den Betroffenen nicht möglich war zu erkennen, welche personenbezogenen Daten zu welchen Zwecken aufgrund welcher Rechtsgrundlage verarbeitet werden. Eine derartige Aufbereitung der Informationen ist nicht ausreichend, um die in Art. 12 f. DS-GVO aufgeführten Informationspflichten zu erfüllen, da es nicht darum geht, die Informationen in irgendeiner Form zur Verfügung zu stellen. Vielmehr sind die in Art. 13 bzw. 14 DS-GVO angegebenen Informationen gem. Art. 12 Abs. 1 DS-GVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln."

3.1.3 Reichweitenmessung

Thematisch nahe an den beschriebenen Fragstellungen zu Datenschutzerklärungen war ein Thermenkomplex, der regelmäßig an den Mediendatenbeauftragten herangetragen wurde, nämlich die Frage nach dem Umgang mit Tools zur Reichweitenmessung auf Webseiten.

Sofern es sich bei den eingesetzten Diensten um solche von Dritten handelt, die die erhobenen Daten auch zu eigenen Zwecken verarbeiten, ist regelmäßig eine Einwilligung des Nutzers erforderlich. Bei selbstgehosteten Diensten, die explizit auch aufgrund der Datensparsamkeit ausgewählt werden und mittels derer auch keine individuellen Nutzerprofile erstellt werden, wie beispielsweise Matomo, ist die Lage jedoch etwas vielseitiger, aber auch komplizierter. Der Einsatz eines Tools ließe sich prinzipiell neben einer Einwilligung auch mit einem berechtigten Interesse gem. Art. 6 Abs. 1 lit. f DS-GVO rechtfertigen, so dass nicht unbedingt eine Einwilligung, sondern lediglich die Möglichkeit eines Widerspruchs erforderlich wäre. Allerdings steht dem die aktuelle Rechtsprechung des BGH entgegen, nach der § 15 Abs. 3 S. 1 TMG als

Umsetzung des Art. 5 Abs. 3 ePrivRL zu lesen ist, und in dieser Eigenschaft gem. Art. 95 DS-GVO die Rechtsgrundlagen der DS-GVO verdrängt. Demnach wäre für jedes technisch nicht erforderliche Cookie mit dieser Zwecksetzung eine Einwilligung einzuholen.

Wie oben unter 2.2.2 dargestellt, war das TMG für den Rundfunk nie unmittelbar, sondern nur über § 47 Abs. 1 RStV und dann nur entsprechend anwendbar. Da dieser Verweisung durch den Gesetzgeber ausdrücklich mit dem Hinweis, dass sich datenschutzrechtliche Anforderungen künftig aus der DS-GVO unmittelbar ergeben würden, aufgehoben wurde, liegt nach der Auffassung des Mediendatenbeauftragten im Rundfunkdatenschutz keine Umsetzung der ePrivacy Richtlinie mehr vor, die nach Art. 95 DS-GVO Regeln der DS-GVO wie dessen Art. 6 Abs. 1 lit. f verdrängen könnte. Die oben geschilderte Vorgehensweise ist daher im Rundfunk möglich.

Da mit dem unter 2.1 bereits erwähnten TTDSG alsbald doch noch eine Umsetzung der ePrivRL in nationales Recht erfolgen soll, wäre die Rechtslage dann neu zu bewerten.

Zu der Thematik gingen auch etliche Beschwerden ein, auf die unter 3.2.7 eingegangen wird.

3.1.4 Zugriffs- und Löschkonzepte

Aufgrund einer grundlegenden Anfrage eines Anbieters aus dem Jahr 2019, inwieweit dessen vorhandenes Konzept zu Zugriffsbeschränkungen und Löschungsvorgaben durch den Mediendatenbeauftragten als ausreichend eingestuft würde, waren bereits im letzten Berichtszeitraum zahlreiche Gespräche geführt und erhebliche Vorarbeiten geleistet worden.

In diesem Berichtszeitzaum fand schließlich ein mehrteiliger Workshop unter Beteiligung mehrerer Mitarbeiter beider Seiten statt, der auf diesen Vorarbeiten aufbauend eine Vielzahl von Verarbeitungszwecken und Speichergesichtspunkten bis ins Detail erörterte und analysierte. Auf diese Weise konnte die durchaus komplexe Datenhaltungsstruktur wie auch das Zugriffs- und das Löschkonzept durch den Anbieter grundlegend weiterentwickelt werden.

3.1.5 Medienprivileg

Das Datenschutzrecht geht seit jeher und so auch die DS-GVO davon aus, dass die Verarbeitung personenbezogener Daten durch Dritte entweder einer Einwilligung des Betroffenen oder einer anderen Rechtsgrundlage bedarf, die die konkrete Verarbeitung zu bestimmten, vorher festgelegten Zwecken erlaubt. Diese Zielsetzung kollidiert ebenso seit jeher mit der üblichen Arbeitsweise von Rundfunk und Presse einerseits wie auch mit deren verfassungsrechtlich vorgegebenem und geschütztem Funktionsauftrag andererseits. Da sich die beiden insoweit entgegengesetzten Rechtspositionen jeweils auf verfassungsrechtliche Vorgaben wie auch

Grundrechtspositionen berufen können, kann eine Lösung nur in einem wertenden Ausgleich dieser Positionen bestehen.

Dieses Spannungsverhältnis einer solchen Lösung zuzuführen dient seit jeher das sogenannte Medienprivileg, das mit der Einführung der DS-GVO mit Blick auf den Anwendungsvorrang des Europarechtes einer Neuregelung bedurfte.

Seit dem 25.05.2018 sind die Regelung der DS-GVO verbindlich anzuwenden, sodass jeder Verantwortliche für die Verarbeitung personenbezogener Daten Dritter einer entsprechenden Rechtsgrundlage in der Regel aus Art. 6 Abs. 1 DS-GVO bedarf, erheblichen Informationsverpflichtungen gegenüber den individuell Betroffenen zu genügen und deren Rechte zu gewährleisten hat; zudem unterliegt er bei Verstößen gegen diese Regeln erheblichen Haftungsverpflichtungen wie auch der Drohung mit empfindlichen Geldbußen.

Da sich bei der Anwendung dieser Regeln auf die Tätigkeit von Journalisten das oben geschilderte verfassungsrechtliche Dilemma ergibt, wird den Mitgliedstaaten in Art. 85 Abs. 1 DS-GVO aufgegeben, das Recht auf Schutz der personenbezogenen Daten mit den Vorgaben der Rundfunk- und Pressefreiheit in Einklang zu bringen. Zu diesem Zweck wird den Mitgliedstaaten andererseits das Recht eingeräumt, von den meisten Vorgaben der DS-GVO Ausnahmen für die Verarbeitung von Daten zu journalistischen Zwecken vorzusehen, wenn dies für den angestrebten Rechtsausgleich erforderlich ist. Hiervon hat der deutsche Gesetzgeber für den Rundfunk zunächst in § 9c RStV und dann in dem diesen ablösenden § 12 MStV[23] einen sehr weitgehenden Gebrauch gemacht.

Dies führt dazu, dass es für die Verarbeitung personenbezogener Daten zu journalistischen Zwecken keiner weiteren darüber hinausgehenden Rechtsgrundlage bedarf, die diese Zwecke verfolgenden Personen lediglich das in § 12 MStV niedergelegte Datengeheimnis zu beachten haben, und den Betroffenen anstelle der Rechte der DS-GVO lediglich die in § 12 Abs. 2 und 3 MStV genannten Rechte zustehen.

Diese Vorgaben schränken die Betroffenenrechte mit Blick auf den Schutz der Rundfunkfreiheit sehr weitgehend ein und räumen selbst das ansonsten grundlegende Recht auf Auskunft, welche Daten über sie gespeichert sind, nur solchen Personen ein, die bereits durch eine Berichterstattung in ihren Persönlichkeitsrechten beeinträchtigt wurden. Vor einer solchen Berichterstattung besteht keinerlei Auskunftsrecht und nach einer solchen auch nur dann, wenn durch die Berichterstattung Persönlichkeitsrechte beeinträchtigt wurden und zudem durch das Auskunftsrecht die Funktionsfähigkeit des Rundfunks nicht in bestimmter Weise erschwert oder eingeschränkt wird.

23 Ergänzend ist für die Ausgestaltung des Medienprivilegs Art. 20 Abs. 6 S. 2 BayMG und für den Bereich der Telemedien der vormalige § 57 RStV, nun § 23 MStV, für die Presse Art. 11 BayPrG und im Übrigen Art. 38 BayDSG zu erwähnen.

Dementsprechend spielt die Frage, ob für Datenverarbeitungsprozesse wie auch für bestimmte Personen das Medienprivileg anwendbar ist, in der Praxis eine durchaus nicht unerhebliche Rolle in unterschiedlichen Zusammenhängen und mit durchaus divergierenden Zielrichtungen.

Da der Medienbeauftragte für den Datenschutz eine der wenigen Datenschutzaufsichtsinstitutionen ist, die sowohl für den gesamten Bereich des üblichen Datenschutzrechtes wie auch für die Anwendung des Medienprivilegs zuständig ist, werden immer wieder Fragen von ganz grundlegenden bis hin zu sehr speziellen Ausgestaltungen an ihn herangetragen.

Neben Anwendungsfolgen im Detail steht vor allem die Frage im Zentrum, wer sich auf das Medienprivileg berufen kann, wofür es letztlich auf den Umstand ankommt, welche Ausgestaltung der Gesetzgeber dem Begriff der journalistischen Zwecke beigeben wollte. Diese journalistischen Zwecke dürften für Personen, die klassische Rundfunkprogramme inhaltlich gestalten, in der Regel klar und eindeutig zu bejahen sein. Schwieriger wird die Beantwortung dieser Frage, wenn man die vom Gesetzgeber in § 54 MStV angesprochenen zulassungsfreien Rundfunkprogramme und damit auch zahlreiche Angebotsformen des Internets mit in den Blick nimmt. Andererseits hat der EuGH vor kurzem festgestellt, dass der Begriff des Journalismus in Anbetracht der Bedeutung, die der Freiheit der Meinungsäußerung in jeder demokratischen Gesellschaft zukomme, weit ausgelegt werden müsse.[24] Der Begriff der journalistischen Tätigkeiten dürfe daher nicht auf Berufsjournalisten beschränkt werden, solange bei einer Äußerung der Zweck im Vordergrund stehe, Informationen, Meinungen und Ideen in der Öffentlichkeit zu verbreiten. Im vom EuGH entschiedenen Fall ging es um eine Aufzeichnung, die der Betroffene auf dem Onlineangebot von YouTube online gestellt hatte.

Diese prinzipielle Sichtweise hat auch der Gesetzgeber des MStV aufgegriffen, der das Merkmal der journalistischen Gestaltung in Beziehung zu einer journalistischen Arbeitsweise setzt und das Tatbestandsmerkmal „journalistisch" funktional deutet, so dass eine berufsmäßige journalistische Tätigkeit hierfür nicht zwingend erforderlich sei.[25]

Andererseits hat der EuGH - wenn auch zu der vormaligen Rechtslage - darauf hingewiesen, dass Ausnahmen und Einschränkungen in Bezug auf den Datenschutz nur in dem Umfang angewandt werden dürften, in dem sie sich als notwendig erweisen, um die fraglichen Grundrechte miteinander in Einklang zu bringen. Dabei sei die Rechtsprechung des EGMR zu berücksichtigen.[26] Ob dies bei der gegenwärtigen deutschen Rechtslage hinreichend geschehen sei, ist unter den deutschen Aufsichtsbehörden durchaus strittig wie auch die Frage, ob die deutsche Rechtslage wegen des Anwendungsvorranges des Europarechts gegebenenfalls ignoriert werden dürfte.

[24] Urteil des EuGH vom 14.2.2019 - C-345/17, Rn.51 ff.
[25] Vgl. Begründung zu § 2 MStV
[26] Urteil des EuGH vom 14.2.2019 - C-345/17, Rn.63 ff.

Von inhaltlicher Bedeutung sind Fragen nach dem Medienprivileg häufig dann, wenn in den angesprochenen Programmen das Persönlichkeitsrecht der dargestellten Personen bzw. derjenigen, über welche berichtet wird, möglicherweise oder vorgeblich beeinträchtigt wurde. In diesen Fällen ergibt sich daher häufig eine gewisse Parallelität zu Fragen des Persönlichkeitsrechtes bzw. der zu beachtenden journalistischen Grundsätze. Da das Persönlichkeitsrecht auf eine reichhaltige Kasuistik und eine langjährige Rechtsprechungstradition verweisen kann, sind diesem Rechtsgebiet häufig maßgebliche Weichenstellungen inhaltlicher Natur zu entnehmen.

3.2 Beschwerden und Kontrollanregungen

Die Anzahl der Beschwerden und Kontrollanregungen ist weiterhin hoch. Zusätzlich wurden deutlich mehr Anfragen von interessierten Bürgern zu Themen wie z.B. eingesetzten Cookies und Tracker auf Websites sowie Fragen zur Zulässigkeit von unterschiedlichsten Formulierungen in Datenschutzerklärungen an uns herangetragen. Dies belegt deutlich, dass das Interesse der Bevölkerung an Datenschutzfragen unvermindert hoch ist. Auffallend ist auch, dass Petenten vermehrt in den diversen Gebieten über ein breites Fachwissen verfügen und dadurch auf konkrete technische Begebenheiten aufmerksam machen. Diese Entwicklung rückt verstärkt technische Sachverhalte in den Fokus. Daraus ergeben sich weitere und höhere Anforderungen an die Fallbearbeitung, die von der Beobachtung der maßgeblichen technischen Entwicklungen und deren Analyse bis hin zum Monitoring von Webseiten und der beweissicheren Dokumentation der entsprechenden Ergebnisse führt.

3.2.1 Auskunftsanspruch

Ein großer Teil der Beschwerden befasste sich mit Auskunftsansprüchen Betroffener über die zu ihrer Person gespeicherten personenbezogenen Daten. Allerdings gab es deutlich weniger Fälle, in denen Anbieter dieser Verpflichtung nicht innerhalb der vorgesehenen Frist nachgekommen sind, als noch im vorangegangenen Berichtszeitraum.

Nach Art. 12 Abs. 3 Satz 1 DS-GVO müssen „Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags“ zur Verfügung gestellt werden. Daher muss eine Auskunft in der Regel unverzüglich – nach nationalem Verständnis ohne schuldhaftes Zögern –, jedenfalls aber innerhalb der Monatsfrist bereitgestellt werden. Die Monatsfrist darf in der Regel nur bei komplexen Sachverhalten ausgeschöpft werden, nicht aber bei Standardfällen.[27] Eine eventuell

27 vgl. Greve, in: Sydow, Europäische DS-GVO 2018, Art. 12 Rn. 24 und Bäcker, in: Kühling/Buchner, DS-GVO/BDSG, 2020, Art. 12 Rn. 33.

erforderliche Fristverlängerung hat der Verantwortliche in jedem Einzelfall zu begründen (Art. 12 Abs. 3 Satz 2, 3 DS-GVO). Diese Vorgaben wurden von den Auskunftsverpflichteten im Berichtszeitraum nicht immer eingehalten. Bei einigen Beschwerde-Fällen musste der Verantwortliche aufgefordert werden, seinen Pflichten fristgemäß nachzukommen und es wurde die fehlende unverzügliche Umsetzung gerügt. In einem Fall wurde ein schriftlicher Hinweis erteilt und weitere technisch organisatorische Maßnahmen vom Mediendatenbeauftragten gefordert, da der eingebundene Auftragsverarbeiter über Monate nicht auf Auskunftsersuchen sowie die Aufforderung zur Löschung von Daten reagiert hatte; die hierfür angeführte Ursache für die nicht erfolgte Erfüllung der Begehren wurde vom Mediendatenbeauftragten als unglaubwürdig eingestuft.

In den meisten Fällen wurde der Rechtsanspruch der Betroffenen auf Auskunft im Anschluss, wenn auch gelegentlich erst nach Einschaltung der Aufsicht, erfüllt.

In unserer Praxis sind die uns zur Kenntnis gelangten Auskunftsanfragen ansonsten in der Regel umfassend beantwortet worden. Grundsätzlich sollte die Auskunft so umfassend sein, dass der Betroffene den Umfang und Inhalt seiner gespeicherten personenbezogener Daten tatsächlich beurteilen kann.

Bei weiteren Fällen hatten die Beschwerdeführer ihre Auskunftsersuchen jedoch als Antwort auf eine vorangegangene Korrespondenz an eine no reply E-Mailadresse gesendet, die nicht für den Empfang von (Antwort-) E-Mails eingerichtet wurde, was in den entsprechenden E-Mails auch so gekennzeichnet war, so dass der Verantwortliche mangels Zustellungsmöglichkeit keine Kenntnis vom Begehren des Betroffenen erhalten konnte.

Häufiger wurden in diesem Berichtszeitraum von Betroffenen auch die Herausgabe von Gesprächsaufzeichnungen von Telefonaten bzw. Anrufprotokollen verlangt.

Der konkrete Inhalt von Auskunftsansprüchen und dem Recht auf Kopie gem. Art. 15 Abs. 3 DS-GVO ist nach wie vor stark umstritten. Pauschale Aussagen zum Umfang und Inhalt dieser Rechte sind daher kaum möglich. Vielmehr kommt es hierfür stets auf den Einzelfall und die Begleitumstände an. Der Auskunftsanspruch soll gem. Erwägungsgrund 63 DS-GVO dem Betroffenen dazu dienen, sich der Verarbeitung personenbezogener Daten bewusst zu sein und deren Rechtsmäßigkeit überprüfen zu können.

Bei Werbeanrufen halten wir die Vorhaltung und Vorlage eines Anrufprotokolls dann für entbehrlich, wenn der Betroffene ergänzende Hinweise erhalten hat, von wem und wie lange er angerufen wurde. Aus datenschutzrechtlicher Sicht scheint es sogar angezeigt, nicht alle Anrufprotokollaufzeichnungen zu speichern, mit den eigenen Systemen zu verknüpfen und vorzuhalten, um den Vorgaben der Datenminimierung und Datensparsamkeit gem. Art. 5 Abs. 1

lit. c, e DS-GVO gerecht werden zu können. Gleichwohl muss ein Nachweis, wer wann wen und warum anrief, gem. Art. 5 Abs. 2 DS-GVO dennoch geführt werden können.

Ob im Einzelfall ein Anspruch des Betroffenen auf Übermittlung von vorhandenen Gesprächsaufzeichnungen in Betracht gezogen werden könnte, wenn der Betroffene explizit Aufzeichnungen herausverlangt, ein Mehrwert für sein Recht auf informationelle Selbstbestimmung besteht, keine Hindernisse entgegenstehen und die Verhältnismäßigkeit für den Verantwortlichen gewahrt wird, kann nicht pauschal beantwortet werden, sondern muss im Einzelfall geprüft werden.

Allerdings ist auch zu berücksichtigen, dass der Verantwortliche ggf. ein Auskunftsverweigerungsrecht gem. § 34 BDSG geltend machen kann.

Sofern jedoch, wie in einigen Fällen, die Gesprächsaufzeichnungen nur zur Qualitätsprüfung angefertigt wurden und nach einer kurzen Speicherfrist gelöscht werden, halten wir es aus Datenschutzgründen nicht für erforderlich und mit dem Gebot der Datenminimierung für nicht vereinbar, derartige Aufzeichnungen nur zu dem Zweck vorhalten zu müssen, eventuelle spezifische Auskunftsanfragen beantworten zu können. Erwägungsgrund 64 DS-GVO geht von einer sehr ähnlichen Wertung aus.

Auch in der Rechtsprechung ist dieses Thema oft Gegenstand von Entscheidungen, die jedoch kein einheitliches Bild vermitteln:

So hat das LG München in einem Fall die Herausgabe von Telefonnotizen/Gesprächsvermerken als Teil der Auskunft und Kopie angesehen:

Art. 15 DS-GVO könne die Betroffenenrechte nur dann gewährleisten, wenn eine entsprechend weite Auslegung erfolge. „Soweit damit in Gesprächsvermerken oder Telefonnotizen Aussagen der Klägerin oder Aussagen über die Klägerin festgehalten sind, handelt es sich hierbei ohne weiteres um personenbezogene Daten, welche zu beauskunften sind und über welche der Klägerin eine Kopie zur Verfügung zu stellen ist“ (LG München I, Endurteil vom 06.04.2020, 3 O 909/19, Rn. 95).

Auch das OLG Köln meint, eine Auskunft sei zu sämtlichen weiteren die Person betreffenden personenbezogenen Daten, insbesondere auch Gesprächsnotizen und Telefonvermerken, zu erteilen, welche der Verantwortliche gespeichert, genutzt und verarbeitet habe (OLG Köln, Urteil v. 26.07.2019, 20 U 75/18).

Das LG Köln entschied jedoch, dass der Anspruch aus Art. 15 DS-GVO „nicht der vereinfachten Buchführung" des Betroffenen diene. Schriftverkehr, der dem Betroffenen bereits bekannt sei, müsse somit nicht nochmal ausgedruckt und übergeben werden. Darüber hinaus entschied das LG Köln auch, dass „Vermerke, rechtliche Bewertungen oder Analysen" ebenfalls keine

personenbezogenen Daten i.S.d. Vorschrift darstellten und somit nicht zu beauskunften seien (LG Köln, Teilurteil vom 18.3.2019, 26 O 25/18).

Etwas restriktiver hat den Auskunftsumfang beispielsweise das ArbG Bonn beurteilt (ArbG Bonn, Urteil vom 16.07.2020, 3 Ca 2026/19, Rn. 110):

„Es sind aus dem Sinn und Zweck der Norm keine Umstände ersichtlich, dass über die Information über das gespeicherte Datum hinaus noch eine Herausgabepflicht von Unterlagen bestehen soll, wie der Kläger es mit seinem Antrag verlangt. Sollte also die Beklagte die Aussage eines Betriebsratsmitgliedes über eine vom Kläger veranlasste Hotelbuchung gespeichert haben, so wäre sie verpflichtet, auf ein entsprechend konkretisiertes Auskunftsersuchen des Klägers diese gespeicherten Daten gegenüber dem Kläger offenzulegen. Eine Herausgabe des Protokolls über diese Aussage beinhaltet die Verpflichtung zur Zur-Verfügung-Stellung einer Kopie gemäß Art. 15 Abs. 3 DS-GVO jedoch nicht."

Auch das LG Stuttgart ist in einem neueren Urteil der Ansicht, dass ein Anspruch auf allumfassende Auskunft und Kopie sämtlicher vorhandener Daten mit dem Sinn und Zweck des datenschutzrechtlichen Auskunftsanspruchs nicht vereinbar sei (LG Stuttgart, Urteil vom 4.11.2020,18 O 333/19, Rn. 22, 23, BeckRS 2020, 38735-nicht rechtskräftig). All dies zeigt, dass stets eine Beurteilung anhand des Einzelfalles geboten ist.

Sofern im Rahmen eines Auskunftsersuchens erhebliche Bedenken bestehen, ob die um Auskunft ersuchende Person tatsächlich diejenige ist, die sie vorgibt zu sein, kann ein zusätzlicher Nachweis wie z.B. eine geschwärzte Ausweiskopie erforderlich sein, damit die Auskunft auch an die richtige Person erfolgt.

Eine eindeutige Identifikation erscheint z.B. erforderlich, wenn kein unterschriebenes Auskunftsersuchen, sondern lediglich ein solches per E-Mail vorliegt und zudem die E-Mailadresse keinen Klarnamen aufweist. Ein Verantwortlicher verweigerte in einem solchen Fall daher zu Recht die Auskunft und forderte vor Auskunftserteilung die Nennung des Namens, der Anschrift sowie weiterer Daten zur Identifizierung des angeblich Betroffenen, der die Auskunft begehrte.

Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die einen Antrag gemäß den Artikeln 15 bis 21 DS-GVO stellt, so kann der Verantwortliche zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind (vgl. Art. 12 Abs. 6 DS-GVO). Eine z.T. geschwärzte Kopie des Personalausweises kann als solch eine Information zur Bestätigung der Identität in Betracht kommen.

Werden umfassende Informationen z.B. zu Vertragsunterlagen mit zahlreichen personenbezogenen Daten eingefordert, kann der auskunftspflichtige Verantwortliche

weitergehende Nachweise über die Identität der die Auskunft verlangenden Person anfordern, und wird dies gegebenenfalls je nach Bedeutung der fraglichen Daten sogar müssen. Wir erachteten daher in solchen Fällen die Anforderung einer Ausweiskopie mit Erkennbarkeit von Name, Anschrift, Geburtsdatum und Gültigkeit unter Schwärzung der übrigen Angaben zum Zwecke der Identifikation für vertretbar und geboten. Allerdings sollte die zum Nachweis der Berechtigung vorgelegte Kopie nach einer erfolgten Identitätsüberprüfung vernichtet werden.[28]

3.2.2 Datenlöschung

In einer Reihe von Beschwerden an den Mediendatenbeauftragten wurde moniert, dass zur Datenlöschung nach Art. 17 DS-GVO aufgeforderte Anbieter ihren Löschverpflichtungen nicht bzw. nicht fristgemäß nachgekommen seien, und dass weiterhin personenbezogene Daten aus einem bestehenden oder beendeten Kundenverhältnis vorgehalten würden.

In der Mehrzahl dieser Fälle konnte der Medienbeauftragte für den Datenschutz jedoch feststellen, dass ein Verstoß gegen datenschutzrechtliche Vorgaben der DS-GVO nicht vorlag: Art. 17 Abs. 1 lit. a der DS-GVO sieht zwar eine Löschverpflichtung des Verantwortlichen vor, wenn eine weitere Verarbeitung der Daten der betroffenen Person für den ursprünglichen Zweck nicht mehr notwendig ist. Die Regelung in Art. 17 Abs. 3 lit. b DS-GVO sieht aber eine Ausnahme hiervon für den Fall vor, dass die weitere Verarbeitung der Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, wie beispielsweise gesetzlichen Aufbewahrungsfristen oder auch zur Verteidigung von Rechtsansprüchen (Art. 17 Abs. 3 lit. d DS-GVO). Im Kundenverhältnis können einen Anbieter gesetzliche Aufbewahrungspflichten von sechs bzw. zehn Jahren treffen, welche sich aus steuerlichen und buchhalterischen Vorschriften (§ 147 Abs. 3 AO, § 257 HGB) ergeben, sodass in einem solchen Fall trotz der grundsätzlichen Löschverpflichtung tatsächlich die Löschung erst nach Ablauf der in der Regel mehrjährigen Aufbewahrungspflichten erfolgen kann. Diese für zahlreiche Petenten überraschende Rechtslage ließ sich häufig erst nach Einschaltung der Aufsicht vermitteln.

Gelegentlich halten Verantwortliche die für Betroffenenrechte vorgesehene Monats-Frist des Art. 12 Abs. 3 S. 1 DS-GVO nicht ein. Da es sich hierbei um ein elementares Problem handelt, wurden Verantwortliche auf diesen Verstoß hingewiesen und aufgefordert, technisch organisatorische Maßnahmen zu ergreifen, um die Fristen künftig einzuhalten.

[28] vgl. hierzu die Ausführungen des LDI NRW unter https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Personalausweis-und-Datenschutz/Datenschutz-und-Personalausweis-2019_07.pdf (Stand Juli 2019, Download 21.12.2020).

3.2.3 Cookiebanner und Consent-Tools

Im Laufe des Berichtszeitraumes kam es zu einigen Beschwerden hinsichtlich der Ausgestaltung von Cookie-Bannern und sogenannten Consent-Tools.

Ein kleiner Teil der Beschwerdeführer bemängelte, dass sie sich grundsätzlich durch Cookie-Banner oder jegliche Art von Cookies gestört fühlten. In diesen Fällen wurde den Beschwerdeführern lediglich die Rechtslage erläutert, wonach der Einsatz von Cookies aufgrund mehrerer Rechtsgrundlagen möglich sein könne. Sofern keine weiteren Verdachtsmomente für einen datenschutzrechtlich zu beanstandenden Verstoß vorlagen, wurde in diesen Fällen auf die Einleitung eines weiteren Verfahrens verzichtet.

Der größere Anteil der Beschwerden zum Thema Cookie-Banner bezog sich jeweils auf konkrete Angebote, bei denen nach Ansicht der Beschwerdeführer die Informationspflichten nicht ausreichend erfüllt, kein Widerspruchsrecht eingeräumt oder auch erforderliche Einwilligungen nicht rechtsgültig eingeholt wurden.

Für die Einholung von Einwilligungen und auch für die Verwaltung von Widersprüchen setzen viele Anbieter inzwischen sogenannte Consent-Tools ein. Hier haben sich bei einem Großteil der Anbieter zwischenzeitlich einheitliche Formulierungen auf Basis des „Transparency and Consent Framework 2.0“ (TCF 2.0) des Wirtschaftsverbandes der Onlinewerbebranche „iab“ durchgesetzt. Unabhängig davon, ob die Formulierungen durch das TCF vorgegeben sind, bleibt festzuhalten, dass weiterhin der Anbieter als Verantwortlicher für eine datenschutzrechtlich korrekte Ausgestaltung zu sorgen hat. Das gilt sowohl für die inhaltliche als auch für die optische Gestaltung. So sind beispielsweise Consent-Tools so zu gestalten, dass für den Nutzer erkennbar wird, dass überhaupt und an welchen Stellen Einstellungen vorgenommen werden können. Auch ist dabei zu vermeiden, den Nutzer durch die optische Gestaltung zur Abgabe einer Einwilligung zu verleiten oder gar zu bestimmen. Hier besteht ansonsten die Gefahr, dass es sich im Zweifel nicht um eine rechtsgültige Einwilligung handelt und die Verarbeitung personenbezogener Daten damit ohne Rechtsgrundlage erfolgt.

Im Rahmen der Einholung von Einwilligungen sollte der Verantwortliche auch sicherstellen, dass der Nutzer über den Inhalt und Umfang seiner Einwilligung hinreichend informiert ist. Sollte dies nicht der Fall sein, ist anzunehmen, dass die Einwilligung nicht in „informierter Weise“ erfolgte und daher nicht wirksam ist.

In einigen Fällen konnte festgestellt werden, dass einzelne Dienste Dritter in die Angebote eingebunden waren, die – insoweit häufig sogar in Übereinstimmung mit den Ausführungen der Consent-Tools – als einwilligungsbedürftig einzuordnen waren, die jedoch bereits mit Aufruf der jeweiligen Website geladen wurden. Die Verarbeitung erfolgte somit bereits, ohne dass die auch vom Verantwortlichen für erforderlich gehaltene Einwilligung vorlag. Die Angebote wurden in den monierten Fällen alle nach einem entsprechenden Hinweis durch den

Mediendatenbeauftragten angepasst. Bei weiteren Sachverhaltsermittlungen stellte sich zumeist heraus, dass es sich in der Regel nicht um eine andere Auslegung der datenschutzrechtlichen Vorgaben oder eine bewusste Verletzung derselben, sondern um technische Fehler oder Fehlkonfigurationen handelte. Sofern die in diesem Zusammenhang durch den Mediendatenbeauftragten problematisierten Sachverhalte zeitnah abgestellt wurden, waren nach dem Hinweis keine weiteren aufsichtsrechtlichen Maßnahmen erforderlich.

3.2.4 Werbung trotz Widerrufs

Häufig erreichten uns Beschwerden, weil die Betroffenen von Ihnen als unerfreulich empfundene Zusendungen wie z. B. Newsletter erhalten hatten, obwohl die betroffenen Personen jeweils ihre Einwilligung für den Versand gemäß Art. 7 Abs. 3 DS-GVO widerrufen hatten bzw. bei Direktwerbung dieser gem. Art. 21 DS-GVO widersprochen hatten. In zahlreichen Fällen war ihnen hierüber sogar eine entsprechende Bestätigung durch den Verantwortlichen zugegangen; dennoch erhielten die Petenten Anrufe, Briefe oder E-Mails mit werblichem Inhalt.

Die Verantwortlichen begründeten diesen Fehler häufig mit der Aussage, dass der Widerruf/Widerspruch aufgrund der Vielzahl an eingegangen Anfragen nicht schnell genug bearbeitet und entsprechend vermerkt worden sei. In einigen Fällen war menschliches Versagen die Ursache, da Mitarbeiter schlicht die Anfrage nicht an die zuständige Abteilung weitergeleitet hatten bzw. den Widerruf/Widerspruch vergessen hatten im System zu vermerken bzw. dort einen falschen „Haken" setzten.

Bezüglich dieser Umstände konnten wir auf eine sofortige Abhilfe hinwirken und haben darauf hingewiesen, dass entsprechende organisatorische Vorgänge etabliert werden müssen, damit Widerrufe/Widersprüche auch tatsächlich umgehend eingetragen und berücksichtigt werden. Z. B. muss sichergestellt werden, dass datenschutzrechtliche Anfragen, die an eine Service E-Mail-Adresse geschickt werden, auch entsprechend weitergeleitet und datenschutzrechtlich bearbeitet werden.

In wenigen Fällen waren Hinweise geboten, da Werbung trotz Vorliegens eines Widerrufs/Widerspruchs versandt wurde bzw. der erteilte Widerruf gar nicht bearbeitet wurde; ein Verstoß zumindest gegen Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 DS-GVO und Art. 21 Abs. 3 DS-GVO sowie gegen Art. 12 Abs. 3 i.V.m. Art 21 DS-GVO musste hier festgestellt werden, da keine Rechtsgrundlage zum Zusenden von Werbung bestand bzw. die Widersprüche nicht innerhalb der vorgesehenen Fristen bearbeitet wurden.

Weitere Ursache von Beschwerden war, dass in E-Mails von Newslettern angegebene Abmeldelinks nicht funktionierten oder auf eine Fehlerseite führten. Auf unser Drängen wurden solche technischen Fehler umgehend behoben. Jedenfalls wurden uns danach keine neueren Beschwerdefälle bekannt.

3.2.5 Altersprüfung per Ausweis

In an uns herangetragenen Beschwerden wurden Bedenken geäußert, dass Personalausweisnummern im Rahmen der Nutzung von Rundfunkangeboten abgefragt würden.

Die Verarbeitung der Personalausweisnummern erfolgte hier zum Zwecke der Altersverifikation aufgrund einer rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 lit. c) DS-GVO in Verbindung mit § 5 Abs. 1 Satz 1 mit Abs. 3 Satz 1 Nr. 1 JMStV (Jugendmedienschutz-Staatsvertrag).

Im Rahmen von Online-Mediatheken wird für einen erweiterten Medienbereich die Nummer des Personalausweises vom Nutzer abgefragt. Diese Nummer muss bei der Registrierung nicht zwingend, sondern nur bei einigen Angeboten angegeben werden, die gewissen Altersbeschränkungen unterliegen. Zweck der Abfrage der Personalausweisnummer ist die Altersverifikation des Nutzers aus Gründen des Jugendschutzes. Sofern Anbieter Angebote, die geeignet sind, die Entwicklung von Kindern oder Jugendlichen zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen, verbreiten oder zugänglich machen, haben sie nach § 5 Abs. 1 Satz 1 JMStV dafür Sorge zu tragen, dass Kinder oder Jugendliche der betroffenen Altersstufen diese üblicherweise nicht wahrnehmen.

Dieser Pflicht kann der Anbieter u.a. dadurch entsprechen, dass er technische oder sonstige Mittel ergreift, die die Wahrnehmung des Angebots für Kinder unmöglich macht oder wesentlich erschweren (§ 5 Abs. 3 S. 1 Nr. 1 JMStV).

Aus der Ausweisnummer wurde daher ausgelesen, ob es sich um einen validen Ausweis handelt, sowie das Geburtsdatum; damit wird der Altersüberprüfung Rechnung getragen, so dass das Angebote auch nur an die berechtigte Altersgruppe ausgespielt wird.

Die Übertragung der vom Nutzer einzugebenden Daten erfolgte verschlüsselt, sodass bei der Eingabe kein Zugriff auf die Daten selbst möglich war. Zudem wurden die Informationspflichten erfüllt, indem die Nutzer auf der Registrierungsoberfläche auf die Eingabe der Ausweisnummer aus Gründen des Jugendschutzes hingewiesen wurden und einen Hinweis auf die Datenschutzerklärung erhielten, in der zusätzlich über die Verarbeitung der personenbezogenen Daten informiert wurde.

Sofern der Anbieter die Ausweisnummer nur vorrübergehend und ausschließlich zum Zweck der Überprüfung des Alters aus Gründen des Jugendschutzes verwendet und die Daten anschließend löscht, ist dieses Vorgehen datenschutzrechtlich nicht zu beanstanden. In der Regel sollte beim Verantwortlichen lediglich vermerkt werden, dass der Nutzer die fragliche Altersvorgabe einhält.

3.2.6 Datentransfer in Drittstaat

Der Verein NOYB - European Center for Digital Rights hat öffentlichkeitswirksam im August 2020 angekündigt, 101 Beschwerden gegen in der EU/EWR ansässige Unternehmen einzulegen, da diese Anwendungen wie „Google Analytics" oder „Facebook Connect" auf Ihren Websites verwenden, welche trotz des nicht mehr anwendbaren Privacy Shields (vgl. EuGH Urteil vom 16.07.2020, C-311/18)[29] personenbezogene Daten an Google bzw. Facebook übermitteln ohne in der Lage zu seien, ein angemessenes Schutzniveau für die personenbezogenen Daten der Beschwerdeführer zu gewährleisten.

Vor der Entscheidung des EuGH in der Rechtssache C-311/18 konnte eine Datenübermittlug in die USA auf das EU-US-Datenschutzschild (Privacy Shield) bzw. den dieses betreffenden Durchführungsbeschluss der EU-Kommission[30] gestützt werden. Durch die in dem Urteil erfolgte Feststellung der Ungültigkeit dieses Durchführungsbefugnisses ist eine Datenübermittlung in die USA damit nicht mehr auf Grundlage dieses Abkommens möglich. Das Recht der USA bietet aus Sicht des EuGH kein der EU im Wesentlichen gleichwertiges Schutzniveau.

Auch uns hat im September 2020 eine der 101 Beschwerden erreicht, die gegen einen bayerischen Anbieter erhoben wurde, der eines der genannten Tools von Facebook auf seiner Webseite einsetzt. Aufgrund der nahezu gleichgelagerten Sachverhalte und Beschwerden wurde im EDSA eine Task Force „101 complaints" gebildet, in der Vertreter aus betroffenen Mitgliedsstaaten kooperativ zusammenarbeiten, um ein einheitliches Vorgehen abzustimmen und den Vorgaben der DS-GVO entsprechend ein möglichst einheitliches Datenschutzniveau in der EU herzustellen.

Für die durchzuführenden Anhörungen im Verwaltungsverfahren hat die EDSA Task Force einen Fragenkatalog ausgearbeitet, der auch unserer Anhörung an den Verantwortlichen zugrunde gelegen hat. Da jedoch mit der einheitlichen Anhörung der Verantwortlichen zumeist nicht hinreichend geklärt werden konnte, welche Daten wann und wohin transferiert werden, und in welchem Verhältnis die betroffenen Unternehmen in diesen Verfahren zu Google bzw. Facebook stehen, wurde ein weiterer Fragenkatalog für Google und Facebook erstellt, der durch die Vorsitzemde der Task Force an die betroffenen Unternehmen mit Aufforderung zur Beantwortung verschickt wurde. Das Verfahren dauert derzeit noch an.

[29] EuGH Urteil vom 16.07.2020, C-311/18- Schrems II
http://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=DE
[30] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12.07.2016 gemäß der Richtlinie 95/46/EG über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes

3.2.7 Tracking Tools

Im Berichtszeitraum erreichten den Mediendatenbeauftragten zusätzlich zu den unter 3.2.3 beschriebenen Beschwerden zu Consent-Tools mehrere Beschwerden hinsichtlich konkreter auf Websites eingesetzter *Trackingtools*. In den eingeleiteten Prüfverfahren wurde neben dem Tracking auch die Information der Nutzer über die Datenerhebung und die Gestaltung der – soweit vorhanden – Einwilligungserklärungen einer genaueren Betrachtung unterzogen.

Mittels verschiedener Technologien wie Cookies oder Browserfingerprinting ist es möglich, das Nutzerverhalten auf Websites zu erfassen. Insbesondere Drittanbieter, die auf Websites eingebunden werden, beobachten das Nutzungsverhalten auch über verschiedene Angebote hinweg und erstellen dabei Nutzungsprofile, u. a. für das Ausspielen von personalisierter Werbung. Die Einsatzmöglichkeiten sind aber keineswegs auf diese Zielsetzung beschränkt.

Bei der Einbindung eben dieser Drittanbieter, die die Nutzungsdaten auch für eigene Zwecke verwenden und bei denen es sich daher nicht um Auftragsverarbeiter handelt, ist genau zu prüfen, ob der Nutzer ausreichend über die Verarbeitung informiert wird, auf welcher Rechtsgrundlage die Verarbeitung erfolgt und ob gegebenenfalls eine Einwilligung des Nutzers erforderlich ist.

In der Vergangenheit wurden die Anbieter lediglich auf aus unserer Sicht datenschutzrechtlich problematische Aspekte ihrer Websites hingewiesen und ihnen die Möglichkeit gegeben, ihre Angebote entsprechend anzupassen. Im Berichtszeitraum wurden nun auch Aufsichtsverfahren in diesem Bereich eingeleitet.

In diesem Zusammenhang sei nochmals auf die Orientierungshilfe für Telemedienanbieter der DSK[31] vom März 2019 hingewiesen, der sich der Medienbeauftragte für den Datenschutz inhaltlich angeschlossen hat. Zu diesem Themenkomplex wurden vom Mediendatenbeauftragten im Berichtszeitraum zwei Online-Veranstaltungen zur Fortbildung durchgeführt, um die Anbieter zu sensibilisieren und auf konkrete Probleme in der Praxis hinzuweisen.

3.2.8 Datenweitergabe an Inkassobüros

Auch in diesem Berichtszeitraum bemängelten einige Beschwerdeführer, dass ihre Daten unrechtmäßig Inkassobüros weitergegeben worden seien. Oft wurde auch moniert, dass keine Einwilligung in die Übermittlung an Inkassobüros vorgelegen habe.

Beim überwiegenden Teil dieser Beschwerden konnte festgestellt werden, dass den Übermittlungen tatsächliche Forderungen zugrunde lagen und diese Übermittlungen daher zumeist

[31] https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

rechtmäßig erfolgten. Eine Einwilligung des Kunden für die Datenweitergabe an ein Inkassobüro ist insbesondere dann nicht erforderlich, wenn sie auf die Rechtsgrundlagen der Art. 6 Abs. 1 Satz 1 lit. b) zur Vertragserfüllung oder zumindest lit. f) DS-GVO zur Datenverarbeitung aufgrund berechtigter Interessen des Gläubigers gestützt werden kann.

Die zivilrechtliche Prüfung des Bestehens der maßgeblichen Forderungen stellt dabei eine inzident zu entscheidende Vorfrage dar, zu deren Klärung den Parteien jenseits der datenschutzrechtlichen Prüfung der ordentliche Rechtsweg offensteht. Liegt hier eine verbindliche Entscheidung vor, wird diese vom Mediendatenbeauftragten in seiner datenschutzrechtlichen Bewertung übernommen.

Besteht demnach eine Forderung, steht es dem Verantwortlichen frei, sich eines Inkassobüros zu bedienen, dem die für seine Tätigkeit erforderlichen Informationen zur Verfügung gestellt werden dürfen.

Ein Widerspruchsrecht, wie es gelegentlich von Beschwerdeführern angenommen wird, besteht gegen eine solcherlei rechtmäßige Weitergabe nach den Vorgaben der DS-GVO in der Regel nicht.

Gelegentlich liegen in konkreten Beschwerdeverfahren komplizierte zivilrechtliche Fallgestaltungen vor, bei denen entweder bereits die Entstehung von Ansprüchen zweifelhaft ist, deren Entwicklung unterschiedlich beurteilt werden oder Zweit- und Drittforderungen mit in die Begründung der eigenen Standpunkte eingebracht werden. In derartigen Verfahren kommt dem Medienbeauftragten gelegentlich die Rolle zu, auf die maßgeblichen datenschutzrechtlichen Vorgaben hinzuweisen, ihre Einhaltung einzufordern und gegebenenfalls diese datenschutzrechtlichen Beurteilungen von zivilrechtlichen Annahmen abhängig zu machen.

3.3 Datenpannen

3.3.1 Allgemeines zu Artikel 33 DS-GVO

Die DS-GVO verlangt u. a., dass personenbezogene Daten mithilfe geeigneter technischer und organisatorischer Maßnahmen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, sodass die Daten, ob unbeabsichtigt oder unrechtmäßig, vor Vernichtung, Verlust, Veränderung oder unbefugtem Zugang bzw. Offenlegung geschützt werden.[32] Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn die Sicherheit durch das Kompromittieren von Schutzmaßnahmen verletzt wird.

32 Vgl. Art. 32, 4 Nr. 12, 33 DS-GVO; Workingpaper 250 (WP250): Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 v. 06.02.2018 der Art. 29 Datenschutzgruppe, S. 7.

Schutzziele sind dabei die Vertraulichkeit, die Verfügbarkeit und die Integrität von personenbezogenen Daten.[33] Sobald dem Verantwortlichen eine solche Verletzung bekannt wird – umgangssprachlich wird auch von „Datenpannen" gesprochen – , besteht eine unverzügliche Meldepflicht gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DS-GVO. Eine Ausnahme ist nur möglich, wenn die Verletzung der Schutzziele voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen führt. Der Verantwortliche ist verpflichtet, jedem ersten Hinweis nachzugehen und zu ermitteln, ob tatsächlich eine Datenschutzverletzung vorliegt.[34]

An uns gemeldete Datenpannen bilden einen erheblichen Teil unserer täglichen Arbeit und nehmen viel Zeit in Anspruch, da stets der Einzelfall, die betroffenen Daten und die Umstände, die dazu führten, untersucht werden müssen. In diesem Berichtszeitraum bildeten Meldungen über Fehlversendungen, unbefugte Veränderungen von Bankdaten sowie Phishing-Angriffe und unbefugte Offenlegung von Kundendaten im Darknet den Schwerpunkt.

3.3.2 Fehlversand und Offenlegung von Gehaltsabrechnungen und Provisionsbetrug

Einen großen Anteil gemeldeter Datenpannen gemäß Art. 33 DS-GVO stellten sogenannte Fehlversendungen, also die fehlerhafte Adressierung z.B. eines Briefes oder einer E-Mail dar. Ihnen allen ist gemein, dass ein unberechtigter Dritter personenbezogene Daten einer anderen natürlichen Person erhielt.

Die gemeldeten Datenpannen unterschieden sich hinsichtlich der betroffenen und fehlgeleiteten Unterlagen bzw. Informationen, aber auch hinsichtlich der der jeweiligen Panne zu Grunde liegenden Begebenheiten und Ursachen im Vorfeld. Neben technischen und individuellen Fehlern Einzelner mit unterschiedlicher Ausrichtung sind gewisse Ursachenreihen einerseits in der fälschlichen Angabe von Kontaktdaten durch die Betroffenen selbst oder der fehlerhaften Übernahme unzutreffender Kontaktdaten wie z. B. E-Mailadressen durch Mitarbeiter von Verantwortlichen aufgetreten. Hinsichtlich der fehlgeleiteten Inhalte spannte sich das Spektrum von vergleichsweise unbedeutenden Unterlagen wie Newslettern, denen aber dennoch personenbezogene Daten zu entnehmen waren, über persönliche Vertragsunterlagen mit Hinweisen auf Bank- und Kreditkartendaten, einer fehlgeleiteten Datenauskunft bis zur an die falsche Person adressierten Gehaltsabrechnung.

Bei fehlversendeten Gehaltsabrechnungen wurde der Verantwortliche genauso wie in einem Fall, in dem eine sehr umfassende Datenauskunft versehentlich einer falschen Person geschickt

33 WP 250 der Art 29 Datenschutz-Gruppe, S. 8.
34 WP 250 der Art 29 Datenschutz-Gruppe, S. 14.

wurde, aufgrund des hohen Risikos für die Rechte und Freiheiten der natürlichen Personen, umgehend dazu aufgefordert, die betroffenen Personen gem. Art. 34 DS-GVO zu benachrichtigen, was im Anschluss auch vom Verantwortlichen umgesetzt wurde. Ferner wurden unrechtmäßige Empfänger aufgefordert, die fälschlich erhaltenen Unterlagen an den Verantwortlichen zurückzugeben und über die ggf. erlangten Kenntnisse Stillschweigen zu bewahren.

Festzustellen ist, dass sich die Meldung von Fehlversendungen im Vergleich zum vorherigen Berichtszeitraum annähernd verdoppelt haben.

Die Meldungen erfolgten meistens innerhalb der gesetzlichen Vorgaben, sodass nur in einigen Fällen ergänzende Hinweise erteilt werden mussten.

Allerdings musste gegenüber einem Verantwortlichen zum Jahresende 2020 hin festgestellt werden, dass bei einer nicht unerheblichen Anzahl von Fällen die Bearbeitung von Hinweisen durch Betroffene auf Fehlversendungen zu spät begann, sodass die unverzügliche Bearbeitung dieser Hinweise zweifelhaft erschien. Der Anbieter wurde dementsprechend aufgefordert, technisch organisatorische Maßnahmen zu ergreifen, um eine umgehende Prüfung von eingehenden Hinweisen von Betroffenen zu etablieren, damit ein „Bekanntwerden" i.S.d. Art. 33 DS-GVO von Datenschutzverletzungen und damit eine unverzügliche Meldung schnellstmöglich gewährleistet ist.

Am Ende des Berichtszeitraumes wurde uns ein Vorgang gemeldet, in welchem möglicherweise im Rahmen eines Provisionsbetruges Änderungen an zahlreichen E-Mailadressen von Kunden in der Kundendatenbank eines Verantwortlichen vorgenommen wurden. Nach gegenwärtigem Erkenntnissen hat dies zum einen zu Veränderungen der zu den betroffenen Kunden hinterlegten personenbezogenen Daten geführt und zum anderen die Offenlegung von weiteren Daten bis hin zu Vertragsunterlagen gegenüber unbefugten Dritte mit sich gebracht. Da die Ursachenforschung und die Ermittlung der Folgen einen erheblichen Umfang angenommen haben, dauert das Verfahren noch an.

3.3.3 Verlust von Datenträgern

Auch im Berichtszeitraum stellte sich wieder die Frage, wie mit verloren gegangenen Datenträgern zu verfahren sei.

In allen uns gemeldeten Fällen waren die Datenträger ausreichend verschlüsselt, sodass auf Fragen der einfachen Zugänglichkeit von unberechtigten Dritten zu den Daten nicht in besonderem Maße einzugehen war; auch waren die Daten nicht dauerhaft verloren, da die Daten in Backups gesichert waren. Festzustellen bleibt, dass Datenträger, auf denen

personenbezogene Daten gespeichert sind, stets verschlüsselt sein sollten, damit im Falle eines Diebstahls oder Verlusts ein Schutz vor allzu leichtem unbefugtem Zugriff auf die Daten besteht.

Besondere Bedeutung erlangte dieser Umstand im aktuellen Berichtszeitraum aufgrund von Pandemie bedingten Home-Office-Zeiten, da ein vermehrter Transport von Datenträgern vom Büro ins Home Office und zurück stattfindet und sich damit auch das Risiko erhöht, auf dem Weg diese Datenträger zu verlieren, oder dass diese gestohlen werden. Deshalb hat der Mediendatenbeauftragte auch frühzeitig im Berichtszeitraum unter https://www.blm.de/datenschutzaufsicht/datenschutz-im-home-office.cfm entsprechende Verhaltensregeln für die Arbeit im Home Office veröffentlicht.

Auch wenn ein Verantwortlicher im Einzelfall aufgrund einer Verschlüsselung ggf. keine Verletzung oder kein Risiko für Rechtspositionen Dritter zu erkennen vermag, erachten wir es gleichwohl für sinnvoll, wenn sich der Verantwortliche beim Verlust auch verschlüsselter Datenträger an die Aufsichtsbehörde wendet, um den Vorfall zu melden und sich ggf. mit dieser abzustimmen. So wird der Aufsicht die Möglichkeit gegeben, die Details des Falles selbst einer Würdigung zu unterziehen, da ihr auch entsprechend Art. 34 Abs. 4 DS-GVO die letzte Entscheidung darüber gebührt, die eingesetzte Verschlüsselung[35] und ggf. auch deren Schutzstandard zu bewerten.

3.3.4 Veränderung von Bankdaten

Eine weitere Spielart von Datenpannen stellte Anfang des Jahres 2020 eine Serie von falsch eingetragenen Bankdaten bei Kunden in der Kundendatenbank eines Verantwortlichen dar.

In diesen Fällen wurden durch Kunden mitgeteilte Änderungen bei Bankdaten vorwiegend durch ein automatisiertes System falsch zugeordnet und in der Folge bei anderen Kunden die dortigen Bankdaten manuell überschrieben. Die jeweiligen Mitarbeiter hatten bei der manuellen Eintragung der neuen Bankdaten nicht überprüft, ob die Änderung der Bankdaten auch beim richtigen Kundendatensatz vorgenommen würde, was in einigen Fällen als besonders fahrlässig erschein, da die Namen der betroffenen Kunden in Einzelfällen erheblich voneinander abwichen. Ob zudem auch eine Offenlegung personenbezogener Daten vorliegen könnte, weil im Kunden-Account die Bankdaten eines Dritten einsehbar waren, konnte zwar dahinstehen, da die Daten „maskiert" angegeben wurden (somit in der Regel nur die letzten fünf Ziffern der IBAN einsehbar waren). Zumindest kam es aber zu einer unbefugten Veränderung von personenbezogenen Daten i.S.v. Art. 4 Nr. 12 DS-GVO, da die Daten unbefugt modifiziert wurden und nicht mehr unversehrt waren[36]- die Bankdaten wurden jeweils mit den Daten eines anderen

35 Vgl. Franck, in Schwartmann/Jaspers/Thüsing, Kugelmann, DSGVO/BDSG, 2020, Art. 33 Rn. 36
36 Vgl. Schwartmann/Hermann, in Schwartmann/Jaspers/Thüsing, Kugelmann, DSGVO 2020, Art. 4 Nr. 12 Rn. 230

Kunden überschrieben. In den meisten Fällen konnte der Fehler nur deshalb entdeckt werden, weil es zu fehlerhaften Abbuchungen bei Dritten kam und sich diese daraufhin beschwerten.

Besonders misslich an diesem Vorfall war, dass in fast der Hälfte der Vorgänge die Meldefrist des Art. 33 Abs. 1 S. 1 DS-GVO nicht eingehalten wurde. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen höchstens 72 Stunden nach Bekanntwerden, so ist ihr eine Begründung für die Verzögerung beizufügen. Auch hiervon hat er Verantwortliche keinen Gebrauch gemacht, sodass auch insofern rechtliche Hinweise erforderlich waren.

Da falsch eingetragene Bankdaten gravierende Folgen verursachen können und daher zum Teil ein hohes Risiko für die Rechte und Freiheiten der Betroffenen bestanden haben dürfte (u.a. Kontrollverlust über personenbezogene Daten, finanzielle Schäden; in fast allen Fällen kam es auch zu fehlerhaften Abbuchungen von Konten bei den betroffenen Kunden), wurden die betroffenen Kunden in den meisten Fällen benachrichtigt. Die Fehlabbuchungen wurden flächendeckend rückgängig gemacht. Die Bankdaten wurden in allen Fällen korrigiert.

Im Hinblick auf das Risiko finanzieller Schäden bei den Betroffenen und zur Vermeidung von Fehlbuchungen sollte gerade bei der Eintragung bzw. Änderung von Bankdaten große Sorgfalt an den Tag gelegt werden und immer mindestens der vollständige Name des Kunden sowie weitere Identifikationsmerkmale mit kontrolliert werden.

Auch aufgrund der zahlreichen gleichgelagerten Fälle wurde das betroffene System von Verantwortlichen letztlich vollständig überarbeitet, sodass inzwischen keine automatisierten Zuordnungen zu Kunden mehr erfolgen, wenn eine Bitte zur Änderung von Bankdaten eingeht. Vielmehr haben nunmehr die Kunden ihre Daten selbst in Ihrem Account zu ändern, was die vormals aufgetretene Fehlerquelle abstellen sollte, da Kunden nur Zugang zu ihrem eigenen Datensatz haben. Die Systemanpassung war aufgrund der Vielzahl von Fällen dringend geboten. Seit dieser Anpassung wurden uns keine entsprechenden Vorgänge mehr gemeldet, sodass davon auszugehen ist, dass die maßgebliche Fehlerquelle beseitigt wurde.

3.3.5 Cyberkriminalität

Im Berichtszeitraum wurden neben den oben erwähnten Datenpannen einige gemeldet, die einen guten Überblick über die gegenwärtigen Bedrohungen für personenbezogene Daten durch Internetkriminelle geben.

In einem Fall bemerkte ein Verantwortlicher, dass in seinem Online-Shop eine Reihe verdächtiger Bestellungen aufgegeben und Änderungen in den Kundenprofilen vorgenommen wurden. Eine Auswertung der Log-Dateien zeigte, dass es zur gleichen Zeit auch zu einer Häufung erfolgloser

Login-Versuche gekommen war. Augenscheinlich waren an anderer Stelle erbeutete E-Mail-Adresse/Passwort-Kombinationen im Webshop des Anbieters ausprobiert worden. Bei Kunden, die die gleiche Kombination bei verschiedenen Diensten eingesetzt hatten, war der Login erfolgreich. Die betroffenen Kunden wurden über den Vorfall informiert und die jeweiligen Passwörter geändert. Da der Ausgangspunkt des Vorfalls als solcher nicht in Herrschaftsbereich des Anbieters erfolgte, war eine kausale Sicherheitsverletzung gem. Art 33 Abs. 1 DS-GVO eher zu verneinen. Da es Dritten aber möglich war, Daten im Herrschaftsbereich des Verantwortlichen zu verändern, handelte es sich dennoch in der Gesamtschau um einen meldepflichtigen Vorfall.

Dieser Fall macht deutlich, dass für die Nutzer ein großes Risiko damit verbunden ist, die gleichen Passwörter für mehrere verschiedene Accounts zu verwenden. Es wäre somit einerseits wünschenswert, dass Nutzer soweit als möglich unterschiedliche Zugangsdaten benutzen. Anderseits sollte ein Verantwortlicher dies auch ermöglichen und unterstützen, indem er frei gewählte Nutzernahmen zulässt. Für die meisten Nutzer wäre es mit unverhältnismäßigem Aufwand verbunden, für jedes Onlinekonto z.B. eine eigene E-Mailadresse anzulegen.

Ferner sollte sich jeder Verantwortliche bewusst sein, dass eine Speicherung von Passwörtern im Klartext oder unzureichend verschlüsselt als unzureichende technische Maßnahme i.S.v. Art. 32. Abs. 1 DS-GVO zu werten ist.

In einem ähnlich gelagerten Fall wurde der Verantwortliche über einen von ihm beauftragten externen Dienstleister darüber informiert, dass bei der Recherche auf „Untergrundmarktplätzen" im Darknet eine Liste mit einer großen Anzahl von Kundendatensätzen entdeckt wurde. Die meisten Einträge dieser Liste waren aus vorangegangenen Recherchen bereits bekannt und entsprechend behandelt worden. Es blieb dennoch eine dreistellige Zahl neuer Datensätze mit Passwort-Informationen übrig, die sich bei einer stichprobenhaften Überprüfung als zumindest teilweise valide herausstellten. Die entsprechenden Kunden wurden informiert und die Zugangsdaten geändert. Auch hier war der Verantwortliche selbst nicht für die Datenpanne ursächlich verantwortlich. Vielmehr waren die Datensätze durch Schadsoftware auf den jeweiligen Rechnern der Kunden, die außerhalb des Einflussbereichs des Verantwortlichen lagen, erbeutet worden.

Schadsoftware war auch der Grund für die Meldung einer weiteren Datenpanne. Ein Anbieter stellte den Angriff auf seine IT-Systeme durch einen sogenannten Kryptotrojaner fest. Bei derartigen Angriffen verschlüsselt eine in die eigenen IT-Systeme eingeschleppte Schadsoftware die vorliegenden Daten. Im Anschluss wird die Wiederherstellung dieser Daten nach Zahlung eines „Lösegeldes" in Bitcoin in Aussicht gestellt. Im vorliegenden Fall konnte der Angriff frühzeitig erkannt und bereits verschlüsselte Daten - nach einer Reinigung der Systeme – aus Sicherheitskopien wiederhergestellt werden.

Hier lässt sich gut erkennen, dass eine sinnvoll aufgebaute Backupstrategie ein Unternehmen vor größerem Schaden bewahren kann. Als Ausgangspunkt kann hier die „3-2-1-Regel" dienen: mindestens drei Kopien auf mindestens zwei unterschiedlichen Medien und mindestens eine davon extern gelagert. So ist sichergestellt, dass auch wenn ein Backup in ein lokales IT-System eingebunden und damit ebenfalls für einen Kryptotrojaner erreichbar sein sollte, eine Datenwiederherstellung durch das Offsite-Backup weiterhin möglich ist.

3.4 Website Prüfung

Im ersten Halbjahr 2020 führte der Mediendatenbeauftragte eine datenschutzrechtliche Prüfung von Anbieter-Websites durch. In einem ersten Schritt wurden zunächst stichprobenartig als besonders reichweitenstark eingestufte Websites gesichtet und dann die Prüfung auf 161 TV-Anbieter und 148 Hörfunkanbieter ausgeweitet. In diesem Rahmen wurde untersucht, welche Trackingmechanismen auf den Websites eingesetzt und inwieweit mittels Cookie-Bannern eine Rechtsgrundlage für die Verarbeitung durch die eingesetzten Trackingdienste geschaffen wurde. Eine tiefergehende Analyse der Trackingdienste erfolgte in diesem Rahmen zunächst nicht. Lediglich die Datenschutzerklärungen wurden dahingehend geprüft, ob die darin enthaltenen Informationen sich mit den eingesetzten Trackingdiensten deckten.

Als Ergebnis musste festgestellt werden, dass bereits anhand der durch die Anbieter dargebotenen Informationen ca. 80% der geprüften Websites offensichtliche datenschutzrechtliche Mängel aufwiesen. Einzelne Stichproben zeigten, dass in den meisten Fällen weitere Kritikpunkte in den jeweiligen Datenschutzerklärungen und Consent-Tools zu finden waren.

Die auffälligsten und häufigsten Fehler lagen darin, dass

- einwilligungsbedürftige Tools bereits geladen wurden, bevor eine entsprechende Einwilligung des Nutzers eingeholt wurde,
- explizit abgewählte Tools dennoch geladen wurden,
- keine ausreichenden Informationen an die Betroffenen gegeben wurden,
- Social-Plugins ohne Zwei-Klick-Lösung oder andere Schutzmechanismen geladen wurden, oder
- die Cookie-Banner derart gestaltet waren, dass die darüber eingeholten Einwilligungen bereits die grundlegenden Anforderungen nicht erfüllten.

Um einen Überblick über etwaige Veränderungen und ein daraus abzuleitendes Bewusstsein für datenschutzrechtliche Problemstellungen bei den Anbietern erkennen zu können, wurden einzelne Aspekte im zweiten Halbjahr erneut untersucht.

Dabei konnte festgestellt werden, dass viele Anbieter ihre Websites zwischenzeitlich angepasst haben. Teilweise war dies auf die Einführung von TCF 2.0 zurückzuführen, teilweise aber auch auf eine grundsätzliche Sensibilisierung für datenschutzrechtliche Fragestellungen.

Da auch die unterschiedlichen Datenschutz-Aufsichtsbehörden bisher nicht in allen Punkten Einigkeit darüber erlangt haben, wie Einwilligungen auf Websites konkret ausgestaltet sein müssen, bzw. welche Ausgestaltungsformen als unzureichend anzusehen sind, wurde seitens des Mediendatenbeauftragten bislang darauf verzichtet, die Untersuchungsergebnisse direkt in Aufsichtsverfahren münden zu lassen. Vielmehr wurden die Erkenntnisse an die Anbieter weitergegeben, damit diese ihre Webangebote rechtskonform ausgestalten. Gleichwohl bieten die Erkenntnisse eine Möglichkeit, im Rahmen künftiger Verfahren früheres (Fehl-)Verhalten oder auch erkennbare Bemühungen zur rechtskonformen Gestaltung mit in die Bewertung einzubeziehen.

3.5 Umsetzungs- und Aufsichtsmaßnahmen

Jede Datenschutzaufsichtsbehörde hat nach Art. 57 Abs. 1 lit. a DS-GVO vor allem die Aufgabe, die Anwendung der Regeln der Grundverordnung und darüber hinaus auch des sonstigen Datenschutzrechtes zu überwachen und durchzusetzen. Zu diesem Zweck verfügt auch der Medienbeauftragte für den Datenschutz gemäß Art. 20 BayMG über alle in Art. 58 Abs. 1 bis 5 DS-GVO genannten Befugnisse zur Überwachung und Durchsetzung der Vorgaben der DS-GVO. Dieser umfangreiche Katalog an Befugnissen reicht von den Untersuchungsbefugnissen des Art. 58 Abs. 1 DS-GVO über konkrete Abhilfebefugnisse des Art. 58 Abs. 2 DS-GVO (umfassend die präventive Warnung, die repressive Verwarnung sowie konkrete Anweisungsbefugnisse) bis hin zur Sanktion der Verhängung von Geldbußen nach Art. 83 DS-GVO als „schärfstes Schwert" der nach der DS-GVO vorgesehenen Maßnahmen. Ein Großteil dieser Maßnahmen kann nicht nur gegenüber dem Verantwortlichen, sondern auch gegenüber Auftragsverarbeitern verhängt werden.

Im Berichtszeitraum hat sich der Medienbeauftragte für den Datenschutz seit Inkrafttreten der DS-GVO auch weiterhin und im Schwerpunkt auf seinen Beratungsauftrag konzentriert und von konkreten Abhilfebefugnissen nur zurückhaltend Gebrauch gemacht. Im Dialog mit den seiner Aufsicht unterstehenden Stellen, insbesondere mit den Anbietern und der BLM, hat er auf eine DS-GVO-konforme Umsetzung datenschutzrelevanter Vorgänge hingewirkt.

Soweit auf Beschwerden Betroffener hin Datenschutzverstöße im Raum standen, wurden im gesamten Berichtszeitraum zur Vorbereitung von Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO zahlreiche Anhörungen in Verwaltungsverfahren gegenüber Verantwortlichen und Auftragsverarbeitern durchgeführt.

In den meisten Fällen konnten auch im Berichtszeitraum 2020 bestehende Mängel abgestellt und so eine datenschutzkonforme Verarbeitung schnell wiederhergestellt werden. Darüber hinausgehende datenschutzrechtliche Maßnahmen waren hierfür in der Regel nicht erforderlich.

Bei 31 Fällen erschien es notwendig, gegenüber den Verantwortlichen einen Hinweis nach Art. 58 Abs. 1 lit. d DS-GVO zu erteilen und sie anzuhalten, ihre technisch-organisatorischen Maßnahmen zu prüfen und in Einzelfällen nachzubessern. In einem weiteren Fall wurde durch den Mediendatenbeauftragten beanstandungswürdiger Verstoß festgestellt und eine Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO ausgesprochen.

Von der Möglichkeit der Verhängung von Geldbußen nach Art. 83 DS-GVO hat der Mediendatenbeauftragte im Berichtszeitraum noch keinen Gebrauch machen müssen.

3.6 Beratungstätigkeit und Fortbildungsveranstaltungen

Zu den Aufgaben des Medienbeauftragten für den Datenschutz gehört im Rahmen des allen Aufsichtsbehörden übertragenen Aufgabenkanons nach Art. 57 Abs. 1 DS-GVO, die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten zu sensibilisieren, wie es Art. 57 Abs. 1 lit. d DS-GVO ausdrückt.

Dieser Aufgabe des Sensibilisierens nimmt sich der Mediendatenbeauftragte einerseits im Rahmen der unter 3.1 beschriebenen Anfragen einzelner Verantwortlicher und andererseits durch an die Allgemeinheit gerichtete Veranstaltungen und Veröffentlichungen wahr.

So wurde beispielsweise im Rahmen der Veranstaltung „Media Innovations“ eine Masterclass zum Thema Tracking angeboten. Hier wurde den Teilnehmern, die überwiegend aus Medienhäusern kamen, zunächst erläutert, welche technische Vorgänge hinter Tracking stecken, welche datenschutzrechtlichen Vorgaben es hierzu gibt und welche Fehler in der Praxis auftreten.

Ebenfalls der korrekten Ausgestaltung von Online-Angeboten, wenn auch in deutlich ausführlicherer Form, widmeten sich zwei Workshops für Verantwortliche zur „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“ der DSK. Im ersten Workshop wurden die rechtlichen Voraussetzungen für Internetangebote, insbesondere die Voraussetzungen, die eine wirksame Einwilligung erfüllen muss, die Frage der Anwendbarkeit der Datenschutzregelungen des Telemedien-Gesetzes und die Voraussetzungen und Anforderungen einer Verarbeitung aufgrund berechtigter Interessen erläutert, während der zweite Workshop darauf aufbauend auch auf Fragen der praktischen Umsetzung einging.

Einer ähnlichen Thematik widmete sich ein Vortragsabend für Eltern, der auf Einladung einer Schule erfolgte. Aber während die zuvor genannten Veranstaltungen sich an Verantwortliche richteten und erläuterten, wie Angebote rechtskonform zu gestalten sind, hatte dieser Vortrag

die Zielsetzung, Betroffene über Online-Tracking aufzuklären und ihnen Möglichkeiten aufzuzeigen, dem soweit als möglich entgegen zu wirken und die eigenen Daten zu schützen.

Im Rahmen der Corona-Pandemie setzen Unternehmen vermehrt kurzfristig auf Homeoffice. Insbesondere wenn es Mitarbeitern ermöglicht wird, von zu Hause oder an anderen Orten außerhalb der normalen Büros zu arbeiten, ohne dass dies zuvor intensiv geplant wurde, ergeben sich neue Herausforderungen unter anderem für die Datensicherheit und den Datenschutz im Unternehmen. Um die Verantwortlichen in den Unternehmen und ihre Mitarbeiter zu unterstützen und um potentielle Datenschutzvorfälle im Vorfeld zu vermeiden, veröffentlichte der Mediendatenbeauftragte eine Aufstellung von Hinweisen und Verhaltensregeln.

Diese Hinweise wurden den Mitarbeitern der Landeszentrale zusätzlich in einer internen Fortbildungsveranstaltung präsentiert.

Da die Aufgabenteilung der Datenschutzaufsichtsbehörden in Bayern sowohl Betroffenen als auch Verantwortlichen oftmals nicht klar ist und insbesondere die Existenz des Mediendatenbeauftragten für einige gelegentlich überraschend erscheint, wurden die Zuständigkeiten und Aufgaben für die interessierte Öffentlichkeit aufbereitet und in Form eines Editorials in Heft 9/2020 der ZD (Zeitschrift für Datenschutz) veröffentlicht.

3.7 Zahlen und Fakten im Überblick

Im Folgenden wird abschließend ein kurzer Überblick über den Umfang der bearbeiteten Fälle und dessen Entwicklung gegeben. Der vorliegende Bericht bezieht sich auf den Zeitraum vom 01.01.2020 bis 31.12.2020.

Wie bereits im Vorjahr sind der Beratungsbedarf wie auch die Beschwerden und die Meldungen von Datenschutzverletzungen spürbar angestiegen.

Am Ende des vorangegangenen Berichtszeitraumes waren noch insgesamt 50 Verfahren offen und wurden im aktuellen Berichtszeitraum weiter bearbeitet.

Zu diesen genannten Verfahren kamen im Jahr 2020 insgesamt genau 200 neu eingeleitete Verfahren hinzu.

Maßgeblich hierfür war, dass in 2020 ein deutlicher Anstieg der gemeldeten Datenpannen, von 58 in 2019 auf 104 in 2020 zu verzeichnen war, während die Anzahl der Beschwerden und Kontrollanregungen mit einer Steigerung von 75 auf 77 annähernd unverändert geblieben ist. Ein Grund für diesen Anstieg der Meldung von Datenpannen könnte die stärkere Sensibilisierung der Unternehmen und die Bedeutung sein, die Datenpannen im Berichtszeitraum beigemessen wurde. So könnte möglicherweise auch eine Rolle gespielt haben, dass Datenpannen aus

anderen Bereichen, - die nicht unter unsere Zuständigkeit fielen - zu medialen Großereignissen wurden.

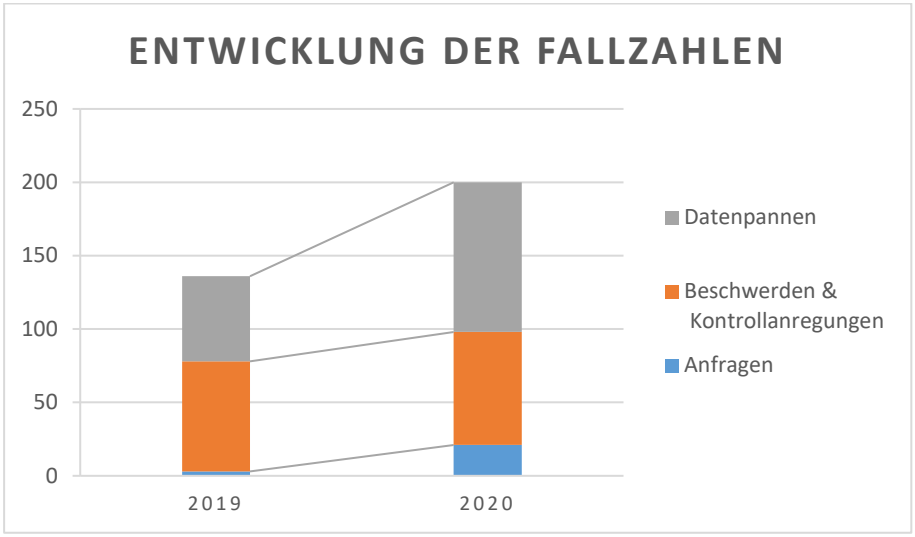
Vorrangig handelte es sich bei den uns gemeldeten Datenpannen um Fehlversendungen, deren Inhalt von belangloseren Werbemails bis hin zu gesamten Vertragsunterlagen, Gehaltsabrechnungen und sogar vollständigen Datenauskünften alles umfasste. Aber auch die sonstige unberechtigte Offenlegung von Daten, Phishingfälle, verlorene Datenträger, Veränderungen von Bankdaten und die Veröffentlichung von Kundendaten im Darknet waren darunter.

Unter dem Stichwort „Beschwerden" werden solche Eingaben geführt, bei denen eine persönliche Betroffenheit des Petenten gegeben ist, während Hinweise aus der Bevölkerung ohne eine individuelle Betroffenheit als „Kontrollanregungen" behandelt werden. In beiden Fällen wird der entsprechende Sachverhalt geprüft und bei einem ausreichenden Anfangsverdacht ein Prüfverfahren eingeleitet.

Daneben gab es auch zahlreiche Beratungsanfragen unterschiedlichster Art. Dabei reichte das Spektrum von Hintergrundgesprächen für eine wissenschaftliche Ausarbeitung bis hin zu Fragen bei der Entwicklung eines unternehmensweiten Löschkonzeptes.

Die Anzahl der Anfragen, die umfangreich genug waren, dass sie zu aktenkundigen Vorgängen führten, belief sich 2020 auf 21. Hinzu kommen allerdings noch zahlreiche weitere Anfragen, die kurzfristig in Ad-Hoc-Beratungen geklärt werden konnten.

Insgesamt wurden 184 Verfahren in 2020 abgeschlossen, nach 119 in 2019; 66 noch offene Fälle wurden ins Jahr 2021 übertragen, wobei in den ersten Wochen des neuen Jahres zahlreiche davon abgeschlossen werden konnten.



3.8 Ausblick

Im Berichtszeitraum lag der Schwerpunkt der Tätigkeit des Medienbeauftragten, nachdem die DS-GVO bereits seit Mai 2018 die verbindliche gesetzliche Richtschnur darstellt, unterdessen bei der Kernaufgabe aller Datenschutzaufsichtsbehörden, die Einhaltung der Datenschutzvorgaben zu überwachen und diese durchzusetzen[37]. Dabei bilden den Ausgangspunkt in aller Regel Beschwerden und Kontrollanregungen betroffener oder besorgter Bürger, die sich häufig selbst um die Einhaltung der Ihnen tatsächlich oder vermeintlich zustehenden Rechtspositionen bemüht haben, mit Ihren Ansichten aber nicht durchdringen und ihre Rechte daher häufig nicht verwirklichen konnten. Da dies aber nach Einschaltung der Datenschutzaufsicht in aller Regel gelingt, handelt es sich hierbei um den Kernbereich des vom Gesetz vorgesehenen Nutzerschutzes, dem daher auch eine entsprechende Aufmerksamkeit gebührt.

Dieser Zielsetzung dient auch die Behandlung von Datenpannen, bei denen die Begleitung durch die Aufsicht einerseits rechtmäßige Zustände wiederherstellen und für die Zukunft sichern, andererseits aber auch die Gewährleistung der von den Datenpannen zumeist betroffenen Nutzerrechte sicherstellen soll.

Daneben bemühen sich der Medienbeauftragte und seine Mitarbeiter nach Kräften, den Anbietern wie auch der Landeszentrale für Beratungen fallspezifisch wie auch abstrakt zur Verfügung zu stehen. Zudem hat sich gezeigt, dass zahlreiche Fragestellungen nicht nur im Einzelfall von Bedeutung sind, sondern zahlreiche Anbieter gleichermaßen betreffen. Und selbst wenn bestimmte Problemfelder für einzelne Anbieter (noch) nicht als relevant erscheinen, kann der Austausch zwischen Verantwortlichen und Aufsicht erheblich dazu beitragen, künftige datenschutzrechtliche Probleme rechtzeitig zu erkennen und möglichst frühzeitig zu entschärfen oder auch zu lösen.

Aus diesen Gründen hat der Medienbeauftragte im Berichtszeitraum mehrere Informationsveranstaltungen vor allem für Anbieter angeboten, in denen aktuelle Datenschutzfragen und die dazugehörigen Rechtsauffassungen der Aufsichtsbehörden und Gerichte dargelegt wurden; zudem soll so auch die Möglichkeit des Austausches unabhängig von konkreten Aufsichtsfällen geboten werden.

Diese Veranstaltungen sollen dabei individuelle Beratungen durch den Medienbeauftragten, wie sie auch die DS-GVO vorsieht, keineswegs ersetzen, sondern stellen ein zusätzliches Angebot dar.

[37] Vgl. Art 57 Abs. 1 lit. a DS-GVO

Neben dem aufsichtlichen Handeln und der Beratung der Verantwortlichen ist auch die Sensibilisierung und Aufklärung der Öffentlichkeit eine Aufgabe jeder Datenschutzaufsichtsinstitution und damit auch des Medienbeauftragten für den Datenschutz, auf die im kommenden Berichtszeitraum ein sich steigerndes Augenmerk zu legen sein wird.

Zudem hat der Medienbeauftragte nach der zunächst vor allem dem Übergang und der Beratung dienenden Phase auch vermehrt Prüfungen durchzuführen, sei es als Folge von Beschwerden oder Kontrollanregungen oder auch anlassunabhängig. Dabei sei nochmals darauf hingewiesen, dass Verantwortliche gemäß Art. 5 Abs. 2 DS-GVO nunmehr einer Rechenschaftspflicht unterliegen, wonach sie nachweisen müssen, dass sie die Vorgaben der DS-GVO eingehalten haben und ihren Verpflichtungen aus Art. 5 Abs. 1 DS-GVO nachgekommen sind.

Da die DS-GVO vor nunmehr fünf Jahren veröffentlicht und in Kraft getreten und seit drei Jahren verbindlich zu beachten ist, lässt sich datenschutz-rechtliches Fehlverhalten nur noch schwerlich länger mit einem Veränderungsprozess begründen. Daher werden künftig Prüfungen und Kontrollmaßnahmen wohl an Bedeutung gewinnen.

Anlasslosen Prüfungen vorgelagert sind anbieterübergreifende Basisuntersuchungen, die bereits in einem gewissen Umfang stattgefunden haben und die Aufgabe haben, einen Überblick über die Marktgegebenheiten im Zuständigkeitsbereich zu vermitteln. Aus diesen Untersuchungen ergeben sich wiederum in erster Linie Aufschlüsse über konkrete Bedarfe für Unterrichtungen und Informationsveranstaltungen, aber auch gegebenenfalls für die Einleitung von Aufsichtsverfahren. Gleichwohl wird die Grundausrichtung der Aufsichtstätigkeit unverändert vor allem darin liegen, die gesetzlichen Vorgaben bekanntzumachen, sie zu erklären, danach aber auch auf deren Einhaltung zu drängen.