3. Tätigkeitsbericht

des

Medienbeauftragten für den Datenschutz

bei der Bayerischen Landeszentrale für neue Medien

(Berichtszeitraum: 01.01.–31.12.2021)

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 für 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.

Der vorliegende Bericht über das Kalenderjahr 2021 soll einen Einblick in unsere Aufgaben und Tätigkeitsfelder liefern und gleichsam auch die Schwerpunkte unserer Arbeit in dieser Berichtsperiode herausstellen. Er ist der dritte des Medienbeauftragten für den Datenschutz, der nach Geltung der Datenschutz-Grundverordnung erstellt wird. Er 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 internationalen Datenverkehr auf der Grundlage des EU-US Privacy-Shield (Schrems II) und die sich daraus ergebenden Folgewirkungen sowie die Entscheidung des Oberverwaltungsgerichts Schleswig-Holstein in Sachen *Facebook*-Fanpages zu nennen. Beide Urteile betreffen zahlreiche Rundfunkanbieter in zentralen Punkten. Auch die vom Europäischen Datenschutzausschuss (EDSA) herausgegebenen Guidelines und die von der deutschen Datenschutzkonferenz (DSK) herausgegebenen Orientierungshilfen nahmen Einfluss auf die aktuellen Entwicklungen.

Weiterhin zentral für unsere Tätigkeit war unsere Teilnahme an den auf europäischer Ebene eingerichteten Task Forces „Banner“ und „101 Beschwerden“: Diese wurden ins Leben gerufen, um zwei, zahlreiche Mitgliedstaaten der EU betreffende

Beschwerdewellen des vom Datenschutzaktivisten Max Schrems gegründeten österreichischen Vereins noyb – European Center for Digital Rights[1] gegen Datenschutzverletzungen von (großen) Unternehmen koordiniert zu begegnen und auf europäischer Ebene eine einheitliche Aufsichtspraxis zu gewährleisten.

Im Anschluss erläutern wir unsere Aktivitäten anhand von Fallbeispielen: Neben Anfragen zum Thema *One Stop Shop*, zur Reichweitenmessung, zu Kondolenzschreiben und zum Medienprivileg beschäftigten uns zahlreiche Beschwerden und Kontrollanregungen, wie beispielsweise zu den Themen Auskunftsanspruch, Datenlöschung, *Cookie Banner*, *Consent*- und *Tracking Tools*, Werbung trotz Widerrufs, Datenverarbeitung im Rahmen eines Unternehmensverkaufs sowie Datentransfer in Drittstaaten. Schließlich nahmen die Meldungen der Verletzung des Schutzes personenbezogener Daten, sogenannte Datenpannen, häufig aufgrund von Fehlversendungen, Veränderung von Bankdaten und Provisionsbetrug wie auch in Verbindung mit Aktivitäten der Cyberkriminalität einen großen Teil unserer Aufsichtstätigkeit ein.

Der Blick auf die Überprüfung von Websites, auf Umsetzungs- und Aufsichtsmaßnahmen und unsere Beratungstätigkeiten und Fortbildungsveranstaltungen leitet über zu Zahlen und Fakten zu unseren Tätigkeiten. Diese liefern eine abschließenden Zusammenfassung und gehen zum Ausblick ins neue Jahr 2022 über.

München, 26.09.2022

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

[1] Das Akronym noyb leitet sich von folgendem Satz ab: My Privacy is None of Your Business.(www.noyb.eu)

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[2].

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: dort aus verfassungsrechtlichen Gründen 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 (jedenfalls im Bereich der DS-GVO) 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.

[2] Hier ist der Anbieterbegriff nach der Legaldefinition des Art. 2 Abs. 2 Satz 1 BayMG gemeint.

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 wohl „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 des Bayerischen Datenschutzgesetztes (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 besondere Schwierigkeiten und waren daher immer wieder ein maßgebliches Thema, da diese im Datenschutzrecht üblicherweise nach dem Sitzlandprinzip entschieden werden. Weil aber unter der Geltung des alten Rundfunkstaatsvertrages

(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, konnte das Sitzlandprinzip insoweit nicht zur Anwendung kommen. Mit dem Übergang zum Medienstaatsvertragt (MStV) hat sich der Gesetzgeber nun auch beim Rundfunk für die Anwendung des Sitzlandprinzips entschieden,[3] für bereits bestehende Zulassungen und Genehmigungen jedoch die Fortführung der alten Zuständigkeiten nach RStV angeordnet.[4] 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 und seine Mitarbeiterinnen und Mitarbeiter[5] im Berichtsjahr auch an unterschiedlichen Terminen zum Erfahrungsaustausch mit anderen (Datenschutz-)Aufsichtsbehörden teil:

Bedeutsam waren vor allem die beiden Sitzungen des Arbeitskreises Medien (AK Medien) der DSK im Februar und im September 2021. Darüber hinaus war der Mediendatenbeauftragte ab Juli 2021 an einer Arbeitsgruppe („AG TKG-Novelle – TTDSG") des AK Medien beteiligt, deren Aufgabe die Vorbereitung auf den Rechtsübergang zum Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) und insbesondere die Entwicklung einer aktualisierten „Orientierungshilfe Telemedien" (vgl. 2.3) für die DSK war. Zu diesem Zweck fanden zwischen August und Dezember 2021 insgesamt sieben Online-Sitzungen in großer Runde und weitere Beratungen statt. Hinzu kam die Beteiligung des Mediendatenbeauftragten am institutionalisierten Austausch der DSK mit den spezifischen Aufsichtsbehörden[6], 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 sowie mit Behörden anderer Mitgliedsstaaten

[3] Vgl. § 106 MStV
[4] Vgl. § 119 Abs. 1 S. 1 MStV
[5] 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.
[6] Der Begriff der spezifischen Aufsichtsbehörden 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 umfasst.

ab. Dies erfolgte in zahlreichen Fällen insbesondere bei Beschwerdewellen[7] zu den Themenbereichen Drittlandtransfer und Dark Pattern[8] [9] sowie zum Einsatz von *Tracking Tools*.

Im Hinblick auf die europaweit eingelegten 101 Beschwerden[10] des österreichischen Vereins noyb zum Einsatz von „Google Analytics" und/oder „Facebook Connect" bei größeren Webseitenanbietern fand mit den anderen betroffenen Behörden ein regelmäßiger Austausch über das weitere Vorgehen statt. Wie im letzten Bericht bereits erwähnt wurde beim Europäischen Datenschutzausschuss (EDSA) auch eine Task Force für diese sogenannten 101 Beschwerden eingerichtet, um eine einheitliche Vorgehensweise und Rechtsanwendung auch auf europäischer Ebene zu gewährleisten. An deren Sitzungen beteiligt sich eine Mitarbeiterin des Medienbeauftragten für den Datenschutz regelmäßig (vgl. hierzu ausführlicher unter 3.2.5).

Darüber hinaus hat der Verein noyb im Berichtsjahr eine weitere Beschwerdewelle initiiert: 422 Beschwerden zum Themenkomplex Dark Pattern wurden verteilt über diverse europäische Datenschutzaufsichtsbehörden eingereicht. Der Mediendatenbeauftragte hat bis zum Redaktionsschluss fünf dieser Beschwerden in seinem Zuständigkeitsbereich erhalten.

Insgesamt hatte noyb hierzu 422 gleichgelagerte Beschwerden in zahlreichen Mitgliedsstaaten der EU erhoben. Zur Erlangung einer abgestimmten Vorgehensweise wurde beim EDSA eine Task Force („Banner") eingerichtet, an der der Medienbeauftragte für den Datenschutz stets durch eine Mitarbeiterin vertreten war (vgl. hierzu ausführlicher unter 3.2.3.)

Begleitend zu diesen Vorgängen fanden laufend inhaltliche Beratungen unter den beteiligten deutschen Aufsichtsbehörden zu den jeweils anstehenden Datenschutzthemen statt und im Herbst 2021 zudem ein Abstimmungsprozess zu den aus zahlreichen ähnlich gelagerten Beschwerden sich ergebenden Beschwerdewellen,

---

[7] Mit dem Begriff der Beschwerdewelle bezeichnen wir zahlreiche weitgehend ähnliche Beschwerden, die einem bestimmten Beschwerdegrund und -gegenstand folgen und zeitlich zusammengefasst abgegeben werden oder weitgehend zeitgleich auftreten.

[8] Die Beschwerden befassen sich alle in unterschiedlicher Ausprägung mit der Frage der konkreten Gestaltung von Einwilligungen und *Cookie Bannern*. Hierbei entsteht der Eindruck, dass die Gestaltung dieser Banner die Nutzer möglichst dazu verleiten soll, umfassende Einwilligung in die Verarbeitung ihrer Daten zu erteilen, wobei bestritten wird, dass diese Folge wirklich gewünscht werde. Beispiele sind irreführendes Farbdesign oder versteckte Auswahlmöglichkeiten zu Einstelloptionen, sogenannte Dark Pattern.

[9] Dies bedeutet wörtlich übersetzt dunkle Muster. Im Kontext dieses Berichtes wird dieser Begriff für Gestaltungsformen auf Internetseiten und Social-Media-Plattformen verwendet, die Nutzer dazu verleiten sollen, unbeabsichtigte, ungewollte und potenziell schädliche Entscheidungen zur Verarbeitung ihrer personenbezogenen Daten zuzulassen. Dunkle Muster zielen darauf ab, das Verhalten der Nutzer zu beeinflussen, und können deren Fähigkeit behindern, ihre personenbezogenen Daten wirksam zu schützen und bewusste Entscheidungen zu treffen.

[10] Das Gemeinsame der Beschwerden liegt in den Datentransfers ins nichteuropäische Ausland, die durch bestimmte in die angesprochenen Datenverarbeitungsprozesse eingebundene Tools ausgelöst werden.

deren Einfluss auf die Aufsichtstätigkeit der Datenschutzbehörden und den künftigen Umgang mit solchen.

Im Berichtsjahr 2021 wurde zudem der informatorische Meinungsaustausch mit der Verbraucherzentrale Bayern fortgeführt. Den Schwerpunkt bildete auch dabei die Gestaltung von *Cookie Bannern*.

Im Hinblick auf eine geplanten BayMG-Novelle hatte der Mediendatenbeauftrage auch im Berichtszeitraum zusammen mit der Landeszentrale wieder auf einige Änderungsbedarfe hingewiesen, die jedoch bisher im Gesetzgebungsverfahren leider noch keine Berücksichtigung gefunden haben.

2. Interessante Entwicklungen im Fokus

2.1 Wichtige gesetzliche Neuerungen

Da auch im Berichtsjahr 2021 auf EU-Ebene die Verhandlungen für eine ePrivacy-Verordnung für den Datenschutz in der elektronischen Kommunikation nicht weiter vorangekommen waren, so dass die ePrivacy-Richtlinie aus dem Jahr 2002[11] bis heute gilt, sah sich der deutsche Gesetzgeber bemüßigt, die deutsche Rechtslage dann doch noch an die bereits seit 2009 geltenden EU-Vorgaben[12] anzupassen. Diese standen zudem auch im Zentrum einer BGH-Entscheidung aus dem Jahr 2020, die die bis dahin eigentlich fehlende Umsetzung in Deutschland durch richterliche Rechtsfortbildung ersetzte.[13]

Forciert wurde dieser Anpassungsdruck durch die Richtlinie 2018/1972/EU des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, die auch eine Änderung des Telekommunikationsgesetzes (TKG) erforderlich machte.

Neu geschaffen wurde daher nun das „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien" (TTDSG) vom 23. Juni 2021 (BGBl. 2021 I 1982), mit dessen Inkrafttreten zum 1. Dezember 2021 zeitgleich ein neues TKG und Änderungen des Telemediengesetzes (TMG) wirksam wurden. Mit dem neuen Gesetz sollte ausweislich der Gesetzesbegründung (BT-Drs. 19/27441, S. 30) eine geschlossene und von den Bestimmungen des Telemediengesetzes und des Telekommunikationsgesetzes getrennte gesetzliche Reglung zum Datenschutz und zum Schutz der Privatsphäre in der Telekommunikation und bei Telemedien geschaffen werden. Die vormaligen Datenschutzbestimmungen des TMG und des TKG einschließlich der Bestimmungen zum Schutz des Fernmeldegeheimnisses wurden aufgehoben, in einem neuen Gesetz zusammengeführt und dabei auch die Anforderungen der DS-GVO aufgenommen.

Das TTDSG enthält unter anderem Vorgaben zum Schutz der Privatsphäre bei Endeinrichtungen und insbesondere Anforderungen bei Speicherung von Informationen in Endeinrichtungen der Endnutzer und für den Zugriff auf Informationen, die bereits in Endeinrichtungen der Endnutzer gespeichert sind – und zwar unabhängig

[11] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).
[12] ePrivacy-Richtlinie in der Fassung, die sie durch die Änderung durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (sog. „Cookie-Richtlinie") erhielt; bedeutsam ist insbesondere die Neufassung von Art. 5 Abs. 3 der ePrivacyRiL.
[13] Urteil des BGH vom 28.05.2020, Az. I ZR 7/16 („Cookie-Einwilligung II"); vgl. hierzu näher 2. Tätigkeitsbericht des Medienbeauftragten für den Datenschutz (S. 14 ff.).

davon, ob die dort gespeicherte Informationen einen Personenbezug aufweisen oder nicht. Gemeint sind hier vor allem der Einsatz von Cookies und ähnlichen Trackingmechanismen, die von Anbietern oftmals zu Analyse- und Werbezwecken eingesetzt werden.

Die zentrale Vorgabe zum Umgang mit solchen Informationen findet sich in § 25 Abs. 1 Satz 1 TTDSG: Danach sind die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Nutzers und die Einwilligung haben nach den Vorgaben der DS-GVO zu erfolgen. Das bedeutet unter anderem, dass der Nutzer seine Einwilligung aktiv und vor dem Beginn der beabsichtigten Verarbeitung erteilen muss. Es ist also nicht ausreichend, wenn der Nutzer eine bereits vorangekreuzte Checkbox erst wieder abwählen muss.

Diese Einwilligung ist nach § 25 Abs. 2 TTDSG nur unter zwei alternativen Voraussetzungen entbehrlich: Nämlich dann, wenn (1.) der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder (2.) die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Trotz der engen Anlehnung des deutschen Gesetzgebers an den Wortlaut der Privacy-Richtlinie gibt es heftige Diskussionen insbesondere zur Auslegung der eben genannten zweiten Ausnahme-Alternative vom Einwilligungserfordernis: Was bedeutet „unbedingt erforderlich" und was ist unter einem „vom Nutzer ausdrücklich gewünschten Telemediendienst" zu verstehen? Während Vertreter der Online-Werbewirtschaft hier einen eher weiten Anwendungsbereich propagieren, haben sich die deutschen Aufsichtsbehörden darauf verständigt, dem Charakter des Art. 25 Abs. 2 TTDSG als Ausnahmevorschrift Rechnung zu tragen und daher die gesetzlichen Voraussetzungen der Ausnahme eng zu verstehen. Zudem ist die im Gesetz genannte unbedingte Erforderlichkeit mit Blick insbesondere auf die der deutschen Regelung zugrundeliegenden europäischen Vorgaben vor allem technisch zu verstehen. Dieses Verständnis des Gesetzes wurde im Dezember 2021 kurz nach

Inkrafttreten des TTDSG in einer ausführlichen 33-seitigen Orientierungshilfe[14] zusammengefasst und veröffentlicht.

2.2 Urteile des EuGH zum EU-US Privacy-Shield und des OVG Schleswig-Holstein zu Fanpages: Folgen und Herausforderungen für die Aufsichtspraxis

2.2.1 Internationaler Datenverkehr („Schrems II") / Standardvertragsklauseln

Auch in diesem Berichtszeitraum entfaltete das Urteil des EuGH vom 16.07.2020[15], in dem sich der EuGH durch seine große Kammer zum zweiten Mal zur Frage geäußert hat, unter welchen Voraussetzungen ein Datentransfer aus dem europäischen Rechtsraum in die USA zulässig ist, große Bedeutung und beschäftigt Verantwortliche, Betroffene sowie Aufsichtsbehörden intensiv. Zudem wurden zur Umsetzung des Urteils zahlreiche Maßnahmen und Vorgaben 2021 beschlossen.

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 verfolgt damit die Zielsetzung sicherzustellen, dass das durch europäisches Recht vorgegebene Schutzniveau für natürliche Personen nicht untergraben wird.[16] Die Übermittlung personenbezogener Daten in Drittländer ist daher nur zulässig, wenn die in Kapitel 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"[17] in den USA unter bestimmten Voraussetzungen ein vergleichbares Schutzniveau bilden würden. Diese Entscheidung der EU-Kommission hatte der EuGH in einem Urteil vom 06.10.2015[18], das sich auf ein Verfahren von Max Schrems gegen die irische Datenschutzaufsichtsbehörde (DPC) bezog, für ungültig erklärt.

---

[14] Diese Orientierungshilfen sind auf der Website der DSK unter folgendem Link zu finden: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html (zuletzt abgerufen am 06.09.2022).
[15] Urteil des EuGH vom 16. Juli 2020 (Rechtssache C 311/18 – „Schrems II").
[16] Vgl. Art. 44 S. 2 DS-GVO.
[17] Weitere Informationen finden sich in folgendem Dokument des Bundestags: https://www.bundestag.de/resource/blob/408314/e1f93c6da6ff2d5da97d7a50b898b4fc/PE-6-074-13-pdf-data.pdf (zuletzt abgerufen am 23.09.2022).
[18] Urteil des EuGH vom 6. Oktober 2015 (Rechtssache C-362/14 – „Schrems I").

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[19] wurde in dem oben genannten Urteil vom 16.07.2020 abermals im Hinblick auf ein 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 so 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 gerichtlich durchzusetzen. Das EuGH Urteil von 2020 stellte hierzu fest, dass auch der im EU-US Privacy Shield-Abkommen vorgesehene Ombudsmechanismus entgegen den Feststellungen der Kommission den betroffenen Personen keinen Rechtsweg bietet, 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 erforderlichen Vorgaben und gegebenenfalls auch 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

[19] Durchführungsbeschluss (EU) 2016/1250.

Schutzniveaus darstellen, sogenannte *supplementary measures*, die am 18.06.2021 nochmals angepasst wurden.[20]

Ferner hat die Europäische Kommission mit Durchführungsbeschluss 2021/914 vom 4. Juni 2021 neue Standardvertragsklauseln erlassen und am 07.06.2021 veröffentlicht[21]. Die neuen Standardvertragsklauseln[22] sind modular aufgebaut und befassen sich mit Übermittlungen von personenbezogenen Daten in Drittstaaten, also Staaten außerhalb des Europäischen Wirtschaftsraumes.

Die Verwender der Klauseln müssen darauf achten, dass zum 27. 12. 2022 die letzte Frist für eine Umstellung auf diese neuen Bedingungen abläuft und bis dahin alle Altverträge auf die neuen Klauseln umgestellt werden. Zu beachten ist stets, dass neben den Standardvertragsklauseln gegebenenfalls auch zusätzliche weitere Maßnahmen zu ergreifen sind, um bei einem Transfer von personenbezogenen Daten in einen Drittstaat das Schutzniveau der EU zu erhalten.

2.2.2 OVG Schleswig-Holstein – Urteil Facebook Fanpage

Mit seinem Urteil vom 25.11.2021[23] stellte das OVG Schleswig-Holstein bislang offene sowie umstrittene Fragen bezüglich einer gemeinsamen Verantwortlichkeit und dem Vorliegen von personenbezogenen Daten im Anwendungsbereich der DS-GVO klar. Bis es jedoch zu einer Entscheidung kommen konnte, bedurfte es des Instanzenzuges bis hin zum EuGH und zurück nach Schleswig-Holstein. Mit dieser Rechtsprechung scheint nun für Rechtsklarheit gesorgt worden zu sein.

Nach Einlegung einer Datenschutzbeschwerde beim Unabhängigen Landeszentrum für Datenschutz (ULD) ordnete dieses an, dass die Wirtschaftsakademie Schleswig-Holstein GmbH (Wirtschaftsakademie) ihre sogenannte Facebook-Fanpage wegen Verstößen von Facebook abschalten musste. Als Beschwerdegrund wurden datenschutzrechtliche Verstöße gegenüber der Wirtschaftsakademie geltend gemacht, die von Facebook ausgehen sollten. Daraufhin erhob die Wirtschaftsakademie im Jahre 2013 Klage zum Verwaltungsgericht und begehrte erfolgreich die Aufhebung des Bescheides. Nachdem die 2014 vom ULD eingelegte Berufung vor dem Oberverwaltungsgericht erfolglos blieb, ging es zur Revision an das Bundesverwaltungsge-

[20] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (europa.eu).
[21] Amtsblatt EU L 199/37.
[22] Diese differenzieren zwischen Übermittlungen von Verantwortlichen an Verantwortliche, von Verantwortlichen an Auftragsverarbeiter, von Auftragsverarbeitern an Auftragsverarbeiter und von Auftragsverarbeitern an Verantwortliche.
[23] OVG Schleswig-Holstein, Urteil vom 25.11.2021 – 4 LB 20/13.

richt (BVerwG). Dieses legte vor einer eigenen Entscheidung zunächst einen Fragenkatalog zur Verantwortlichkeit von Fanpagebetreibern und zur Anwendbarkeit des deutschen Datenschutzrechts dem Europäischen Gerichtshof im Vorabentscheidungsverfahren vor. Im Anschluss an das Urteil des EuGH vom 05.06.2018[24] hob das BVerwG 2019, die Entscheidung des OVG Schleswig-Holstein aus dem Jahre 2014 auf und verwies den Streit an das OVG zurück. Das OVG hat nun mit Urteil vom 25.11.2021 einen schwerwiegenden Datenschutzverstoß in der Verwendung der personenbezogenen Daten von Facebook-Nutzern festgestellt:

Zu einem Verstoß gegen die DS-GVO komme es laut OVG jedenfalls dann, wenn Registrierungsdaten von Facebook-Nutzern mit den übrigen vorhanden Daten (nämlich IP-Adressen und/oder Cookies) aufgrund des Fanpage-Aufrufes ohne vorherige Einwilligung verknüpft und verwendet werden, um sogenannte Insight-Statistiken zu erstellen sowie den Aufruf der Fanpage in einem Profil zu speichern und zu Werbezwecken zu nutzen. Denn diese Vorgänge würden weder der Inanspruchnahme noch der generellen Funktionsfähigkeit der Fanpage oder des Facebook Netzwerkes dienen (Rn. 124).

Das OVG kommt unter anderem zu dem Ergebnis, dass auch dynamische IP-Adressen eine Personenbezogenheit aufweisen können (Rn. 92, 103). Zwar beziehe sich eine dynamische IP-Adresse nicht als Information auf eine „bestimmte natürliche Person". Jedoch gehe aus dem Wortlaut von Art. 2 lit. a) Datenschutz-Richtlinie hervor, dass nicht nur eine direkt identifizierbare, sondern auch eine indirekt identifizierbare Person als bestimmbar angesehen werde (Rn. 103). Hierfür müssten sich auch nicht alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden. Es reiche, wenn die Verknüpfung – auch mit Hilfe Dritter – zu einer Bestimmung der betreffenden Person führe. Mit selbiger Argumentation nimmt das OVG eine Personenbezogenheit auch für die von Facebook genutzten c_user-Cookies an (vgl. Rn. 93, 103).

Eine gemeinsame Verantwortlichkeit für die Verstöße nahm das OVG nach Einbeziehung der Vorabentscheidung des EuGHs im konkreten Fall für die Wirtschaftsakademie und Facebook an (Rn. 142). Zwar führe eine gemeinsame Verantwortlichkeit nicht zwingend auch zu einer gleichwertigen Verantwortlichkeit, so dass die Wirtschaftsakademie als Fanpage-Betreiberin für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die sie weder Zwecke noch Mittel (gemeinsam mit Facebook) festlege, nicht als im Sinne von Art. 2 lit. d) Datenschutz-Richtlinie verantwortlich angesehen werden kann (Rn. 147). Wie bereits in seinem Fashion-ID-

[24] EuGH, Urteil vom 05.06.2018 – C 210/16.

Urteil[25] festgestellt, kann laut EuGH die Frage der gemeinsamen Verantwortlichkeit nicht für alle vage in Zusammenhang stehende Datenverarbeitungen zwangsläufig einheitlich beantwortet werden, sondern muss vielmehr im Hinblick auf jeden konkreten Datenverarbeitungsvorgang differenziert geprüft werden (Rn. 66). Da die Wirtschaftsakademie jedoch einen maßgeblichen Beitrag zur Entscheidung über die Mittel der Verarbeitung personenbezogener Daten dadurch geleistet habe, dass sie mit der Einrichtung ihrer Fanpage Facebook überhaupt erst die entsprechende Datenverarbeitung ermögliche (Rn. 150), komme auch ihr eine (Mit-)Verantwortung zu. Auch über die Zwecke der maßgeblichen Datenverarbeitung habe sie jedenfalls stillschweigend mitentschieden, indem sie die Fanpage derart eingerichtet hat, dass es bei ausreichender Frequentierung zwingend zur Er- und Bereitstellung einer Insights-Statistik komme. Offen gelassen hat das OVG die rechtliche Einordnung von weiteren Cookies sowie die Frage, ob und inwieweit eine Datenübertragung bei Einbindung von *Social Plug-ins* in Webseiten außerhalb des Facebook-Netzwerks mit einem Besuch der Fanpage verbunden ist (Rn. 158).

2.3 Guidelines und 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 07/2020 on the concepts of controller and processor in the GDPR vom 02.09.2020 Version 2.0 Adopted on 07 July 2021
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (from 10.11.2020)
- Guidelines 01/2021 on Examples regarding Personal Data Breach Notification Adopted vom 14.12.2021 (1. Version vom 14.1.2021)
- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR vom 18.11.2021

Auch die DSK und die Europäische Kommission haben unter anderem folgende Orientierungshilfen und wichtige Papiere veröffentlicht:

- Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021)

[25] EuGH, Urteil vom 29.07.2019 – C-40/17.

- Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021 (Stand: 16. Juni 2021): Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail
- neue Standardvertragsklauseln der Europäischen Kommission mit Durchführungsbeschluss 2021/914 vom 4. Juni 2021 erlassen und am 07.06.2021 veröffentlicht (Amtsblatt EU L 199/37).

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

Einige der bei der Landeszentrale zugelassenen Anbieter haben ihre Unternehmensstruktur so eingerichtet, dass Datenverarbeitungstätigkeiten an Tochtergesellschaften ausgelagert sind, die ihren Sitz auch außerhalb Bayerns haben können. Die ausgelagerten Tätigkeiten betreffen z. B. Kundenakquise, Nutzerverwaltung usw. Nicht immer bestehen ausdrückliche Auftragsverarbeitungsverhältnisses nach Art. 28 DS-GVO zwischen Mutter- und Tochtergesellschaft, was die Frage nach der örtlich und sachlich zutreffenden Datenschutz-Aufsicht aufwirft.

Da der Rundfunkdatenschutz im Grundsatz auf erteilten Rundfunkzulassungen bzw. -genehmigungen aufbaut, spielte der Sitz eines Unternehmens bisher für die sektorspezifische Zuständigkeit des Medienbeauftragten zunächst keine bestimmende Rolle anders als im allgemeinen Datenschutzrecht, das das Sitzlandprinzip generell anwendet. Dennoch sind auch im Rundfunkdatenschutz die europarechtlich vorgegebenen Regeln des sogenannten One-Stop-Shop-Verfahrens zu beachten.[26] Dies gilt insbesondere für Verarbeitungsverfahren, die als grenzüberschreitend im Sinne von Art. 4 Nr. 23 DS-GVO anzusehen sind, da dann gegebenenfalls Aufsichtsbehörden anderer Mitgliedstaaten der EU an den fraglichen Verfahren zu beteiligen sind.

In der konkreten Aufsichtspraxis wurden Fragestellungen zum One-Stop-Shop-Verfahren im Berichtszeitraum in unterschiedlichen Zusammenhängen 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 hierbei auch Veränderungen in der Konzern- bzw. Unternehmensstruktur oder bei Akquisitionen. Von Bedeutung ist häufig auch der

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

Deutschland, Österreich und die Schweiz verbindende gemeinsame Sprachraum, weshalb der Mediendatenbeauftragte einen Austausch mit der Österreichischen Datenschutzbehörde pflegt.

3.1.2 Reichweitenmessung

Die Frage nach dem Umgang mit Tools zur Reichweitenmessung auf Webseiten (auch in Verbindung mit der Implementierung über Consent-Management Plattformen, vgl. hierzu näher 3.2.3) war ein Themenkomplex, der im Berichtszeitraum regelmäßig an den Mediendatenbeauftragten herangetragen wurde.

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 solchen Tools ließe sich – bei alleiniger Betrachtung unter dem Blickwinkel der DS-GVO – 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 stand dem – auch schon vor Inkrafttreten des TTDSG zum 01.12.2021 – die aktuelle Rechtsprechung des BGH aus dem Jahr 2020 entgegen, nach der § 15 Abs. 3 S. 1 TMG als Umsetzung des Art. 5 Abs. 3 ePrivRL zu lesen ist und in dieser Eigenschaft gemäß Art. 95 DS-GVO die Rechtsgrundlagen der DS-GVO verdrängte. Demnach war und ist für jedes (technisch) nicht unbedingt erforderliche Cookie oder den Zugriff auf die Endeinrichtung des Nutzers mit dieser Zwecksetzung eine Einwilligung einzuholen. Eine Ausnahme vom Einwilligungserfordernis ist jedenfalls seit Inkrafttreten des TTDSG zum 01.12.2021 nur unter den engen Voraussetzungen des § 25 Abs. 2 TTDSG möglich. Zu Recht weist die OH Telemedien 2021 darauf hin, dass für eine einwilligungsfreie Reichweitenmessung hohe Hürden bestehen, die – neben strengen Kriterien für die Bestimmung der unbedingten Erforderlichkeit – als maßgebliche Kriterien für die Bestimmung des von Endnutzer ausdrücklich gewünschten Telemediendienstes eine granulare Festlegung erfordern, für welche Funktion des Telemediendienstes welcher konkrete Speicher- und Auslesevorgang von Informationen auf dem Endgerät erfolgt.

3.1.3 Mitteilung von Spendern bei Spendenaufrufen zum Zwecke der Bedankung

Bei Geburtstagen, Jubiläen oder ähnlichen Anlässen erbitten die Jubilare bzw. in Trauerfällen die Angehörigen zunehmend anstelle von Geschenken bzw. Blumen oder Kränzen eine Spende an eine ihnen geeignet und förderungswürdig erscheinende Einrichtung. Im Berichtsjahr wurde an uns die Frage herangetragen, ob die geförderte Einrichtung dem Wunsch der ursprünglichen Veranlasser nachkommen dürfe, diese über eingegangene Spenden zu informieren, da diese sich bei den jeweiligen Spendern bedanken möchten.

Die zu den zuwendenden Personen vorliegenden Daten sind allein schon wegen des jeweiligen Namens personenbezogen, so dass eine Weitergabe nur erfolgen darf, wenn hierfür eine entsprechende Rechtsgrundlage vorliegt. In Ermangelung anderer Umstände dürfte hierfür regelmäßig nur eine Einwilligung oder ein überwiegendes berechtigtes Interesse auf Seiten des ursprünglichen Veranlassers in Betracht kommen. Eine Einwilligung wird jedoch häufig daran scheitern, dass nur eine informierte Einwilligung Gültigkeit beanspruchen kann, die dafür erforderlichen Informationen bei dem jeweiligen Spendenaufruf insbesondere bei Todesfällen aber zumeist als unpassend empfunden werden und daher unterbleiben.

Die Annahme eines überwiegenden berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO an der Weitergabe der Daten wird andererseits häufig deshalb verneint, weil es sein könne, dass Spender nicht genannt werden wollten, und zudem mit der Weitergabe der Daten nicht zu rechnen sei.

Gleichwohl erscheint im Gegensatz zu diesen Annahmen eine solche Rechtsgrundlage möglich, sofern der Spendenaufruf mit einer entsprechenden Individualisierung des jeweiligen Anlasses verbunden wird und zudem der Hinweis erfolgt, dass diesen individuellen Anlass nicht mit der Spende verbinden und dort nennen solle, wer anonym bleiben wolle. In dieser Konstellation kann nicht mehr mit Anonymität rechnen, wer die Spende dennoch mit der Nennung des fraglichen Anlasses verbindet, so dass mit der Weitergabe der Daten an den Veranlasser des Spendenaufrufs durchaus zu rechnen wäre. Dies gilt gleichwohl nur für die Weitergabe des Namens des Spenders zum Zwecke eines entsprechenden Dankes, nicht jedoch für die der jeweiligen Höhe der Zuwendung. Zudem sollte die jeweilige geförderte Einrichtung einen entsprechenden Hinweis in ihre Datenschutzerklärung sowie in geeigneter Art und Weise im Umfeld derartiger Spendenaufrufe aufnehmen.

3.1.4 Medienprivileg

Das deutsche 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 verfassungsrechtlich fundierte 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.

Einen solchen Ausgleich zu schaffen ist Sinn und Zweck des sogenannten Medienprivilegs, das mit der Einführung der DS-GVO im Hinblick auf den Anwendungsvorrang des Europarechtes einer Neuregelung bedurfte.

Seit dem 25.05.2018 sind die Regelungen 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, daneben aber auch 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 den Schutz personenbezogener Daten mit den Vorgaben der Rundfunk- und Pressefreiheit in Einklang zu bringen. Zu diesem Zweck wird den Mitgliedstaaten andererseits aber auch das Recht eingeräumt, in einem gewissen Gegensatz zum ansonsten geltenden Vorrang der Vorgaben der DS-GVO Ausnahmen von den meisten dieser Regeln 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[27] einen sehr weitgehenden Gebrauch gemacht.

[27] 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.

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 deutlich zurückhaltenderen, 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.

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 in diesem Zusammenhang 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[28] und damit auch zahlreiche Angebotsformen des Internets mit in den Blick nimmt. Andererseits hatte der EuGH in 2019 festgestellt, dass der Begriff des Journalismus

[28] Zum 01.04.2022 wurde auch im BayMG die Genehmigungsfreiheit für weite Teile des Rundfunks in Bayern eingeführt (vgl. Art. 26 BayMG), so dass ab diesem Zeitpunkt auch insoweit bei neuen Angeboten die Rundfunkgenehmigung nicht mehr erforderlich und damit häufig nicht mehr anzutreffen sein wird und daher als Differenzierungskriterium ausscheiden muss. Allerdings tritt eine Anzeigepflicht an die Stelle der vormalig erforderlichen Genehmigungen.

in Anbetracht der Bedeutung, die der Freiheit der Meinungsäußerung in jeder demokratischen Gesellschaft zukomme, weit ausgelegt werden müsse.[29] 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 der Plattform 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.[30]

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 Europäischen Gerichtshof für Menschenrechte (EGMR) zu berücksichtigen.[31] 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.

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.

Im Berichtszeitraum erlangte erstmals auch das die Kehrseite des Medienprivilegs bildende Datengeheimnis praktische Bedeutung. Den Hintergrund bildet der Umstand, dass die Verarbeitung von Daten zu journalistischen Zwecken die hiermit befassten Personen einerseits in datenschutzrechtlicher Hinsicht sehr weitgehend schützt, andererseits aber auch jede Verarbeitung zu anderen als journalistischen

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

Zwecken untersagt und für Zuwiderhandlungen sogar erhebliche Sanktionen vorsieht. In der Praxis bedeutet dies, dass die Aufnahme einer journalistischen Tätigkeit zu einem bestimmten Sachverhalt die dabei verwendeten und gesammelten Informationen dem oben genannten Datengeheimnis unterwirft und den mit dieser journalistischen Tätigkeit befassten Personen eine sehr weitgehende Geheimhaltungsverpflichtung für alle anderen Zwecke auferlegt.

3.2 Beschwerden und Kontrollanregungen

Die Anzahl der Beschwerden und Kontrollanregungen ist weiterhin hoch. Zusätzlich wurden deutlich mehr ins Detail gehende Beschwerden zu Themen wie z. B. eingesetzte Cookies und Tracker auf Websites sowie Fragen zur Zulässigkeit von unterschiedlichsten Formulierungen in Datenschutzerklärungen und der Gestaltung von Einwilligungs-Bannern an uns herangetragen. Dies belegt nachdrücklich, dass das Interesse der Bevölkerung an Datenschutzfragen unvermindert hoch ist. Auffallend ist auch, dass Petenten vermehrt in diversen Gebieten über ein breites, gelegentlich auch vertieftes Fachwissen verfügen und dadurch neben allgemeinen Beobachtungen auch auf zum Teil nur mit erheblichem Vorwissen erkennbare konkrete technische Begebenheiten aufmerksam machen. Diese Entwicklung rückt verstärkt technische Sachverhalte in den Fokus, die entsprechend technisch geschultes Personal sowohl auf Seiten der Verantwortlichen als auch auf Seiten der Datenschutzaufsicht erforderlich machen. 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. Auffallend zum Ende des Berichtsjahres war, dass vermehrt „Muster-Beschwerden“ oder gar „Beschwerde-Generatoren“ genutzt wurden, die automatisiert eine Vielzahl von gleichartig gelagerten Beschwerden gegen unterschiedliche Beschwerdegegner in kurzer Zeit produzieren. Dies führte auf Aufsichtsseite zu erheblichen Belastungen und letztlich Kapazitätsengpässen, da derartige automatisierte Prozessabläufe bei der Beschwerdebearbeitung beim Medienbeauftragten für den Datenschutz nicht möglich sind und jeder Fall individuell behandelt werden muss, solange er als individuelle Beschwerde eingereicht wird. Es ist davon auszugehen, dass dieses Phänomen von automatisiert generierten Beschwerden noch zunehmen wird.

3.2.1 Auskunftsanspruch

Nach wie vor befasste sich ein Teil der Beschwerden 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.[32] Eine eventuell 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 Beschwerdefällen musste der Verantwortliche aufgefordert werden, seinen Pflichten nachzukommen bzw. durch aufsichtliche Maßnahmen dazu veranlasst werden. In unserer Praxis sind die uns zur Kenntnis gelangten Auskunftsanfragen in der Regel letztlich umfassend beantwortet worden. Grundsätzlich sollte die Auskunft so umfassend sein, dass der Betroffene den Umfang und Inhalt seiner gespeicherten personenbezogener Daten tatsächlich beurteilen kann.

In einigen Fällen akzeptierte der Beschwerdeführer keine elektronische Auskunft, sondern verlangte eine Auskunft in Papierform. Die Frage, in welcher Form eine Beauskunftung zu erfolgen hat, kann nicht pauschal beantwortet werden und ist auch in der DS-GVO nicht zweifelsfrei festgelegt. Ein vollständiges Wahlrecht auf Seiten der betroffenen Person scheidet unseres Erachtens ebenso aus wie ein vollständiges Wahlrecht des Verantwortlichen. Vielmehr sind stets die Umstände des konkreten Einzelfalls und die Zumutbarkeit auf beiden Seiten zu berücksichtigen. In der Regel haben die Verantwortlichen zumindest aus Kulanz auch eine Auskunftserteilung in Papierform ermöglicht, sodass insoweit keine weiteren Maßnahmen erforderlich waren.

Der konkrete Inhalt von Auskunftsansprüchen und des Rechts auf Kopie gemäß Art. 15 Abs. 3 DS-GVO ist seit Längerem stark umstritten. Der Auskunftsanspruch

[32] 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.

soll gemäß Erwägungsgrund 63 DS-GVO dem Betroffenen dazu dienen, den Inhalt und das Ausmaß der Verarbeitung ihn betreffender Daten zu erkennen und deren Rechtmäßigkeit überprüfen zu können.

Anders als im vorherigen Berichtszeitraum gab es weniger Beschwerden zur Herausgabe von Gesprächsaufzeichnungen im Rahmen von Auskunftsersuchen gemäß Art. 15 DS-GVO. Gleichwohl ist das Thema schwierig und arbeitsintensiv, weil es nach wie vor sehr häufig Gegenstand von gerichtlichen Entscheidungen ist, die bisher insgesamt kein einheitliches Bild vermitteln:

So hat das LG München in einem Fall die Herausgabe von Telefonnotizen/Gesprächsvermerken als Teil der Auskunft und Kopie angesehen (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 VG Schwerin urteilt am 29.4. 2021, dass personenbezogene Daten umfassend geschützt werden sollen. Dieser Schutz könne nur konsequent verwirklicht werden, wenn eine Auskunft über die vollständig gespeicherten Daten erteilt werde.[33]

Auch das OLG München[34] möchte den Begriff des personenbezogenen Datums weit verstehen und nicht auf sensible oder private Informationen beschränken. Er umfasse potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, wenn es sich um Informationen über die in Rede stehende Person handle, also wenn die Information auf Grund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft sei. Telefonnotizen, Aktenvermerke und Protokolle als interne Vermerke bei den Beklagten, die Informationen über die Klägerin enthalten, seien ebenfalls als personenbezogene Daten einzuordnen.

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 im Sinne der Vorschrift darstellten und somit nicht zu beauskunften seien (LG Köln, Teilurteil vom 18.3.2019, 26 O 25/18).

[33] VG Schwerin Urteil v. 29.4. 2021 – 1 A 1343/19.
[34] OLG München, Urteil v. 4.10.2021, 2021 – 3 U 2906/20.

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

Durch ein neues BGH Urteil vom 15.06.2021 – Az. VI ZR 576/19 – ergibt sich nun aber wohl eine sehr umfassende Pflicht zur Herausgabe von (Kopien von) personenbezogenen Daten.

Der BGH kommt verkürzt dargestellt zu dem Ergebnis, dass auch interne Vermerke und Kommunikation des Verantwortlichen Teil der verpflichtenden Auskunft gegenüber dem Betroffenen sein können.

Im konkreten Fall hatte der Kläger weitergehende Auskünfte hinsichtlich der gesamten noch nicht mitgeteilten Korrespondenz der Parteien, einschließlich der Daten des vollständigen Prämienkontos und etwaig erteilter Zweitschriften und Nachträge zum Versicherungsschein sowie Datenauskünfte bezüglich sämtlicher Telefon-, Gesprächs- und Bewertungsvermerke von der Beklagten zum Versicherungsverhältnis gefordert (Rn. 21). Der BGH folgt der Ansicht des EuGH, dass der Begriff personenbezogene Daten weit zu verstehen sei (Rn. 22).

Daher könnten „zurückliegende Korrespondenz der Parteien, das "Prämienkonto" des Klägers und Daten des Versicherungsscheins sowie interne Vermerke und Kommunikation der Beklagten (...) nicht kategorisch vom Anwendungsbereich des Art. 15 Abs. 1 DS-GVO ausgeschlossen werden.“ (Rn. 24).

Schreiben des Klägers an die Beklagte seien grundsätzlich ihrem gesamten Inhalt nach als personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO anzusehen. Die personenbezogene Information bestehe bereits darin, dass sich der Kläger dem Schreiben gemäß geäußert habe. Auch die Schreiben der Beklagten an den Kläger sollen dem Auskunftsanspruch insoweit unterfallen, als sie Informationen über den Kläger nach den oben genannten Kriterien enthielten. Dass die Schreiben dem Kläger bereits bekannt sind, schließt für sich genommen entgegen der Auffassung des Berufungsgerichts den datenschutzrechtlichen Auskunftsanspruch nicht aus (Rn 25).

Die Fragen des Umfangs von Auskunftsansprüchen wird uns wohl auch in Zukunft intensiv beschäftigen.

3.2.2 Datenlöschung

Auch im Berichtsjahr 2021 wurde in einer Reihe von Beschwerden moniert, dass zur Datenlöschung nach Art. 17 DS-GVO aufgeforderte Anbieter als Verantwortliche ihren Löschverpflichtungen nicht bzw. nicht fristgemäß nachgekommen seien und dass dort weiterhin personenbezogene Daten aus einem bestehenden oder beendeten Kundenverhältnis vorgehalten würden.

In der Mehrzahl dieser Fälle konnte der Medienbeauftragte für den Datenschutz im Jahr 2021 feststellen, dass ein tatsächlicher Verstoß gegen datenschutzrechtliche Vorgaben der DS-GVO entgegen der Meinung der Beschwerden 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 wegen gesetzlicher Aufbewahrungsfristen oder 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 darf. 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 zur Umsetzung bzw. Benachrichtigung nicht ein. Da es sich hierbei um ein elementares Problem handelt, mussten Verantwortliche aufsichtlich angehalten werden, technisch-organisatorische Maßnahmen zu ergreifen, um die Fristen jedenfalls künftig einzuhalten.

3.2.3 *Cookie Banner* und *Consent Tools*

Im Laufe des Berichtszeitraumes kam es wieder zu einer Reihe von Beschwerden hinsichtlich der Ausgestaltung von *Cookie Bannern* und sogenannten *Consent Tools*.

Der größere Anteil der Beschwerden zum Thema *Cookie Banner* bezog sich auch im Jahr 2021 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 von der Streitfrage, ob die Formulierungen durch das TCF vorgegeben sind oder nicht, 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. *Consent Tools* sind beispielsweise 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. Derartige Gestaltungen stellen letztlich das erforderliche Merkmal der „Freiwilligkeit" der zu erteilenden Einwilligung und damit die Einwilligung insgesamt in Frage, so dass damit die Gefahr entsteht, dass es sich nur wegen dieser Gestaltung nicht um eine rechtsgültige Einwilligung handelt und die Verarbeitung der personenbezogenen Daten ohne Rechtsgrundlage und damit rechtswidrig erfolgt.

In diesem Zusammenhang gab es wie oben bereits erwähnt eine konzertierte Beschwerdewelle des Vereins noyb mit europaweit 422 Beschwerden, von denen fünf in den Zuständigkeitsbereich des Medienbeauftragten für den Datenschutz fallen. Diese Beschwerden richten sich gegen beliebte Webangebote und die Art und Weise wie auch die Form, in der Einwilligungen zur Datenerhebung, Weiterleitung an Dritte und zur späteren Nutzung dieser Daten eingeholt werden. Aus Sicht der Beschwerden werden auf diesen Webseiten die Nutzer unzulässig zu solchen Einwilligungen bewegt. Die Beschwerden befassen sich alle in unterschiedlicher Ausprägung mit der Frage der konkreten Gestaltung solcher Einwilligungsprozesse im Rahmen von *Cookie Bannern*. Die maßgebliche Frage ist, ob die Gestaltung dieser Banner, die Nutzer rechtswidrig dazu verleiten, umfassende Einwilligung in die Verarbeitung ihrer Daten zu erteilen, ohne dass diese dies tatsächlich wollen (sogenannte „Dark Pattern").

Im Zuge dieser über ganz Europa verteilten, weitgehend gleichgelagerten Beschwerden wurde eine Task Force beim EDSA eingerichtet, die die Vorwürfe der Beschwerden gemeinsam diskutieren soll, um ein möglichst harmonisiertes Vorgehen aller betroffenen europäischen Aufsichtsbehörden sicherzustellen.

Im Rahmen der Einholung von Einwilligungen soll der Nutzer über den Inhalt und Umfang der Einwilligung hinreichend informiert werden. 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 auch festgestellt werden, dass einzelne Dienste Dritter in die Angebote eingebunden waren, die – insoweit häufig sogar in Übereinstimmung mit den Ausführungen der vom Verantwortlichen eingesetzten *Consent Tools* – als einwilligungsbedürftig einzuordnen waren, die also vor ihrem Einsatz einer Einwilligung des Betroffenen bedurften. Dennoch werden diese Dienste häufig bereits mit Aufruf der jeweiligen Website geladen, obwohl die dafür erforderliche Einwilligung zu diesem Zeitpunkt keinesfalls vorliegt. Die Angebote wurden in den monierten Fällen nach einem entsprechenden aufsichtlichen Hinweis angepasst. Bei weiteren Sachverhaltsermittlungen stellte sich oftmals allerdings auch heraus, dass es sich nicht um eine Folge einer abweichenden Rechtsauffassung oder gar eine bewusste Verletzung datenschutzrechtlicher Vorgaben, sondern um technische Fehler oder Fehlkonfigurationen handelte. Sofern die in diesem Zusammenhang durch den Mediendatenbeauftragten angesprochenen Sachverhalte zeitnah abgestellt wurden, waren nach dem Hinweis keine weiteren aufsichtsrechtlichen Maßnahmen erforderlich.

3.2.4 Werbung trotz Widerrufs

Wie auch im letzten Berichtszeitraum erreichten uns häufig Beschwerden, weil Betroffene von ihnen als unerfreulich empfundene Kontaktaufnahmen oder 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 bzw. bei Direktwerbung dieser gemäß 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 bzw. E-Mails oder wurden anderweitig Gegenstand werblicher Maßnahmen.

Die Verantwortlichen begründeten diese Vorgänge häufig mit menschlichem Versagen, wie z. B. dass Mitarbeiter schlicht die maßgebliche Mitteilung nicht an die zuständige Abteilung weitergeleitet hätten bzw. vergessen hätten, den Widerruf/Widerspruch im System zu vermerken, oder dort einen falschen „Haken" gesetzt hätten. Oft seien auch technische Fehler die Ursache gewesen.

Bezüglich dieser Umstände konnten wir auf eine sofortige Abhilfe hinwirken und haben angemahnt, dass entsprechende organisatorische Vorgänge etabliert

werden, die sicherstellen, dass Widerrufe/Widersprüche auch tatsächlich umgehend eingetragen und berücksichtigt werden Zudem müssen in solchen Fällen die technischen Systeme entsprechend auf Fehler überprüft werden.

Im Berichtszeitraum ergab sich erstmals das Problem sogenannter Teilwidersprüche, das als solches dann entsteht, wenn ein Verantwortlicher eine einheitliche Rechtsgrundlage für unterschiedliche Verarbeitungsprozesse nutzt, wie z.B. bei einer allgemein gehaltenen Werbeeinwilligung oder bei Direktwerbung auf Basis von § 7 Abs. 3 UWG. In diesem Fall hat die betroffene Person gemäß Art. 21 Abs. 2 DS-GVO das Recht, jederzeit Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogener Daten zum Zwecke derartiger Werbung einzulegen. Wird dieser Rechtfertigungsgrund z.B. zum Versand unterschiedlicher Newsletter verwendet und dementsprechend ebensoviele Verarbeitungsprozesse unterhalten, kann der Betroffene selbstverständlich jeder einzelnen Verarbeitung, bzw. Zusendung von Newslettern individuell widersprechen oder seine Einwilligung insoweit individualisiert widerrufen.

Problematisch wird die Fallgestaltung, wenn der Verantwortliche nur noch den Widerruf oder Widerspruch für jeden einzelnen Verarbeitungsvorgang zulässt, so dass der Betroffene z.B. beim generellen Wunsch, von der Zusendung von Werbung dieses Verantwortlichen verschont zu werden, eine für ihn gegebenenfalls unübersichtliche Vielzahl von Erklärungen abgeben muss, obwohl alle diese Vorgänge letztlich nur auf einem einheitlichen Rechtsgrund beruhen.

Einerseits muss der Widerruf einer Einwilligung nach Art. 7 Abs. 3 S. 4 DS-GVO so einfach sein, wie es die Erteilung war; liegt eine einheitliche Einwilligung vor, muss diese auch einheitlich widerrufen werden können. Andererseits wird die ansonsten mögliche Aufteilung der Berechtigung zur Direktwerbung auf Basis von § 7 Abs. 3 UWG in unterschiedliche Verarbeitungsprozesse dann problematisch, wenn ein einheitlicher Widerspruch nicht bzw. nicht in der vorgesehenen Form möglich ist, oder es an entsprechenden vom Gesetz vorgesehenen Hinweisen für den Betroffenen fehlt. Nach einer entsprechenden Beratung konnten die bestehenden Mängel zumeist abgestellt werden.

In einigen Fällen war auch ein aufsichtliches Vorgehen angezeigt, da Werbung trotz Vorliegens eines Widerrufs/Widerspruchs versandt wurde bzw. der erteilte Widerruf gar nicht bearbeitet wurde; in wenigen Fällen erschien es nötig, einen Verstoß 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 in Verbindung mit Art 21 DS-GVO festzustellen, da keine Rechtsgrundlage zum Zusenden von Werbung bestand bzw. die Widersprüche nicht innerhalb der vorgesehenen Fristen bearbeitet wurden.

3.2.5 Datentransfer in Drittstaaten

Der Verein noyb – European Center for Digital Rights – hat im August 2020 101 Beschwerden gegen in der EU/EWR ansässige Unternehmen öffentlichkeitswirksam eingelegt, 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)[35] personenbezogene Daten an Google bzw. Facebook übermitteln, ohne in der Lage zu sein, ein angemessenes Schutzniveau für die personenbezogenen Daten der Beschwerdeführer zu gewährleisten.

Vor der Entscheidung des EuGH in der Rechtssache C-311/18 konnte eine Datenübermittlung in die USA auf das EU-US-Datenschutzschild (Privacy Shield) bzw. den dieses betreffenden Durchführungsbeschluss der EU-Kommission[36] gestützt werden. Durch die in dem Urteil erfolgte Feststellung der Ungültigkeit dieses Durchführungsbeschlusses ist eine Datenübermittlung in die USA auf Grundlage dieses Abkommens nicht mehr 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 die Task Force „101 complaints" gebildet, in der Vertreter aus zahlreichen EU-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 in 2021 einen neuerlichen Fragenkatalog ausgearbeitet, der die Grundlage auch unserer weiteren Tätigkeit in dieser Angelegenheit bildete. Das bei uns anhängige Verfahren berührt wegen der Einbindung des eingesetzten Facebook Tools und der damit einhergehenden Datentransfers, die letztlich in den USA enden, so viele grundlegende Fragen, dass das Verfahren im Berichtszeitraum nicht abgeschlossen werden konnte, sondern weiterhin andauert, was auch mit den unterschiedlichen beteiligten Datenschutzaufsichtsbehörden zusammenhängt. Die komplexen Frage-

[35] EuGH Urteil vom 16.07.2020, C-311/18- Schrems II
http://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=DE .
[36] 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.

stellungen rund um den Drittlandstransfer werden uns wie auch die anderen Aufsichtsbehörden in den kommenden Jahren weiter beschäftigen.

3.2.6 *Tracking Tools*

Insbesondere gegen Ende des Berichtszeitraums – im Zuge des Inkrafttretens des TTDSG (vgl. oben 2.1) – erreichten den Mediendatenbeauftragten zusätzlich zu den unter 3.2.3 beschriebenen Beschwerden zu *Consent Tools* mehrere Beschwerden hinsichtlich konkreter auf Websites eingesetzter *Tracking Tools*.

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, unter anderem 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 diesem Zusammenhang sei nochmals auf die von der DSK herausgegebene „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021“ (OH Telemedien 2021) hingewiesen, der sich der Mediendatenbeauftragte für den Datenschutz inhaltlich angeschlossen hat.

3.2.7 Datenweitergabe an Inkassobüros

Wie auch in den letzten Berichtszeiträumen 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 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 solche 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 bei denen Zweit- und Drittforderungen mit in die Begründung der eigenen Standpunkte eingebracht werden. In derartigen Verfahren kommt dem Medienbeauftragten häufig die Rolle zu, auf die maßgeblichen datenschutzrechtlichen Vorgaben hinzuweisen, ihre Einhaltung einzufordern und gegebenenfalls diese datenschutzrechtlichen Beurteilungen von zivilrechtlichen Annahmen abhängig zu machen.

3.2.8 Datenverarbeitung im Rahmen eines Unternehmensverkaufs

Im Berichtszeitraum gingen zahlreiche Beschwerden zu einem Unternehmensverkauf bei uns ein, in dessen Zuge einer unserer Anbieter einen bisherigen Unternehmensteil an einen dritten Erwerber verkaufte. Alle Beschwerden waren nahezu identisch gelagert und befassten sich mit der Frage, ob eine Kontaktaufnahme des bisherigen Unternehmens mit den Betroffenen datenschutzrechtlich zulässig war und ob die weitere Datenverarbeitung durch das neue Unternehmen möglich wäre. In den uns vorliegenden Fällen hatte der Anbieter den Verkauf des Unternehmens allen Kunden vorab per E-Mail mitgeteilt und darauf hingewiesen, dass, sofern nicht binnen einer konkreten Frist ein Widerspruch eingehe, alle Verträge und Daten an das neue Unternehmen übermittelt und dort weiterverarbeitet würden. Dies geschah in Form der Mitteilung einer Änderung der AGBs per Mail an alle Kunden. Das vertraglich vereinbarte inhaltliche Angebot sollte uneingeschränkt fortgeführt wer-

den, so dass die Ausgestaltung, die Art und der Umfang der Datenverarbeitung weiterlaufen würden.

Die Verwendung der Kontaktdaten zur Mitteilung über die bevorstehende AGB-Änderung erachteten wir in diesen Fällen als eine wichtige, das Vertragsverhältnis betreffende Information, so dass die Verarbeitung der entsprechenden personenbezogenen Daten der Nutzer der Erfüllung der bestehenden vertraglichen Verpflichtungen gemäß Art. 6 Abs. 1 lit. b) DS-GVO diente und so auch datenschutzrechtlich zulässig war.

Für Kunden, die der AGB-Änderung widersprachen, erfolgte keine Übergabe von Daten an den Käufer des Unternehmens. Rechtsgrundlage der Übermittlung der Daten der Kunden, die der AGB-Änderung zustimmten und damit das Vertragsverhältnis mit dem Erwerber des Unternehmens und neuem Anbieter der vertraglichen Leistungen fortführten, war vorliegend Art. 6 Abs. l lit. b DSGVO, da die Kundendaten zur Fortführung der bestehenden Verträge der Kunden erforderlich seien. Kunden hätten sich nach dem Unternehmensübergang weiterhin im Account einloggen und Inhalte buchen können. Alle Beschwerdeführer haben jedoch der Weitergabe ihrer Daten an das neue Unternehmen widersprochen, sodass es gar nicht erst zu einer Datenübermittlung kam; stattdessen wurden diese Verträge beendet und die Accounts vor dem Wirksamwerden der Folgen des Unternehmensverkaufs gelöscht, sodass wir im Rahmen der Beschwerden auch nicht über die grundsätzliche Frage der Möglichkeit einer weiteren Nutzung von Bestandsdaten durch den Käufer des Unternehmens entscheiden mussten.

3.3 Datenpannen

3.3.1 Allgemeines zu Meldungen nach Artikel 33 DS-GVO

Sobald dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten 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.[37]

[37] WP 250 der Art 29 Datenschutz-Gruppe, S. 14.

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 zur Verletzung führten, untersucht werden müssen. In diesem Berichtszeitraum bildeten erneut Meldungen über Fehlversendungen und unbefugte Veränderungen von Bankdaten, aber auch Meldungen im Zuge der Microsoft Exchange Zero-Day Lücke den Schwerpunkt.

3.3.2 Fehlversand 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 wie Anschrift, Telefonnummern oder Geburtsdatum zu entnehmen waren bis hin zu Bank- und Kreditkartendaten.

Festzustellen ist, dass die Zahl der Meldungen von Fehlversendungen sich weiterhin auf einem ähnlich hohen Niveau wie im Vorjahr bewegt.

Die Meldungen erfolgten zumeist innerhalb der gesetzlichen (Frist-)Vorgaben, sodass nur in einigen Fällen Hinweise erteilt werden mussten.

Gewisse Schwierigkeiten bestehen aber nach wie vor, Hinweisen hier auf Fehlversendungen unverzüglich nachzugehen, wie es das Gesetz vorsieht, und dementsprechend rechtzeitig in die Bearbeitung der sich daraus ergebenden möglichen Datenpannen einzutreten. In einer nicht unerheblichen Anzahl von Fällen begann die Bearbeitung von Hinweisen durch Betroffene erkennbar zu spät, sodass Hinweise und gelegentlich auch Aufforderungen erforderlich waren, technisch organisatorische Maßnahmen zu ergreifen, um eine umgehende Prüfung von eingehenden Hinweisen und damit eine wie vorgesehen unverzügliche Meldung von Datenschutzverletzungen sicherzustellen.

Auffallend war in 2021 ein weiterer Anstieg von sogenannten „Identitätsdiebstählen", die häufig im Rahmen von mutmaßlichen Provisionsbetrügereien erfolgten. Wie in unserem letzten Bericht bereits angedeutet, hat sich nunmehr der Verdacht verdichtet, dass in einer Reihe von Fällen wohl Mitarbeiter eines Dienstleisters im Namen Dritter Verträge abgeschlossen haben, um für abgeschlossene Verträge jeweils Vermittlungsprovisionen zu erhalten. Die Verwendung der Kundendaten war dabei von den betroffenen Kunden nicht veranlasst und gegen deren Willen erfolgt.

Im Rahmen der Prüfung der Meldung von Datenschutzverletzungen war im Zuge unserer Aufsichtstätigkeit eine anwachsende Anzahl gleich gelagerter Fälle aufgefallen, die eine zufällige Entstehung der gemeldeten Probleme zunehmend unwahrscheinlich erscheinen ließ. Nachfragen beim betroffenen Unternehmen und unsere Aufforderung, dem oben genannten Verdacht nachzugehen, führten letztlich zur Aufdeckung dieser Serie von sehr wahrscheinlichen Betrugsfällen. Im Rahmen der Untersuchung durch den betroffenen Anbieter weitete sich die Anzahl der wahrscheinlich involvierten Mitarbeiter des fraglichen Dienstleisters ebenso erheblich aus wie die Anzahl der betroffenen Kunden, die unterdessen wohl auf eine deutlich 4-stellige Zahl angewachsen ist.

In diesem Zusammenhang sei die Zusammenarbeit mit dem involvierten und mutmaßlich ursächlichen Auftragsverarbeiter beendet worden. Alle betroffenen Kundendaten seien jedoch umfassend vom Verantwortlichen überprüft und berichtigt worden. Die Ermittlungen beim Verantwortlichen dauerten nach wie vor ebenso noch an wie auch zivil- und strafrechtliche Verfahren. Nach Beendigung dieser Verfahren werden auch wir eine abschließende datenschutzrechtliche Würdigung vornehmen.

3.3.3 Veränderung von Bankdaten

Eine weitere Spielart von Datenpannen stellt auch in diesem Berichtsjahr die falsche Eintragung von Bankdaten bei Kunden in der Kundendatenbank eines Verantwortlichen dar.

In solchen Fällen werden zumeist durch Kunden mitgeteilte Änderungen seiner Bankdaten durch ein automatisiertes System falsch zugeordnet und in der Folge bei anderen Kunden die dortigen Bankdaten überschrieben, oder der jeweilige Mitarbeiter hat bei einer manuellen Eintragung der neuen Bankdaten nicht überprüft, ob die Änderung der Bankdaten auch beim richtigen Kundendatensatz vorgenommen wird. In diesen Fällen kommt es in der Regel daher zu einer unbefugten Veränderung von personenbezogenen Daten im Sinne von Art. 4 Nr. 12 DS-GVO, da die Da-

ten unbefugt modifiziert wurden und nicht mehr unversehrt sind[38], weil sie mit den Daten eines anderen Kunden überschrieben wurden.

Im Hinblick auf das Risiko finanzieller Schäden bei den Betroffenen und zur Vermeidung von Fehlbuchungen muss gerade bei der Eintragung bzw. Änderung von Bankdaten große Sorgfalt an den Tag gelegt und immer mindestens der vollständige Name des Kunden sowie weitere Identifikationsmerkmale mit kontrolliert werden. Verantwortliche werden bei derartigen Sorgfaltspflichtverletzungen ermahnt, ihre Prozesse datenschutzkonform auszugestalten.

3.3.4 Cyberkriminalität: Microsoft Exchange Zero-Day Lücke

Im Berichtszeitraum wurden neben den oben erwähnten Datenpannen einige gemeldet, die einen Einblick in die laufenden Bedrohungen für personenbezogene Daten durch Internetkriminelle geben. Besonders hervorzuheben ist ein maßgebliches Softwareproblem:

Am 03.03.2021 hatte Microsoft die Existenz von vier Zero-Day-Lücken in lokal (on premise) betriebenen Exchange-Servern offiziell bestätigt und entsprechende Sicherheitsupdates veröffentlicht. Die Lücken wurden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Bedrohungsstufe 4 „sehr hoch" bewertet. Die Lücken ermöglichen es Angreifern, unter bestimmten Umständen auf Informationen zuzugreifen, die auf den Servern abgelegt sind (E-Mails, Adressbücher, Kalender etc.) sowie beliebigen Code auf den Servern zu schreiben und auszuführen. Es gab Hinweise, dass die Sicherheitslücke durch eine „Hafnium" genannte Hackergruppe bereits aktiv ausgenutzt worden war. In einigen Fällen wurde dabei Software hinterlegt, die einen Zugriff auch nach Beheben der eigentlichen Sicherheitslücke ermöglichen sollte. Daneben war von Sicherheitsforschern ein öffentlich verfügbares Exploit entdeckt worden, sodass Angriffe wohl nicht mehr nur auf diese eine Hackergruppe beschränkt waren.

Im Zuge dieser Sicherheitslücke und erfolgter Meldungen veröffentlichte der Mediendatenbeauftragte auf seiner Website Verhaltenshinweise[39] für betroffene Verantwortliche mit weiterführenden Links und wies in diesem Zusammenhang auf die grundsätzliche Meldepflichtigkeit nach Art. 33 DS-GVO hin.

---

[38] Vgl. Schwartmann/Hermann, in Schwartmann/Jaspers/Thüsing, Kugelmann, DSGVO 2020, Art. 4 Nr. 12 Rn. 230.
[39] Diese sind zu finden unter https://www.blm.de/datenschutzaufsicht/exchange_luecke.cfm (zuletzt abgerufen am 15.09.2022).

3.4 Website Prüfung

In 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.

Als Ergebnis musste gleichwohl 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,
- erforderliche Zwei-Klick-Lösung oder andere Schutzmechanismen fehlten oder
- die *Cookie Banner* derart gestaltet waren, dass die darüber eingeholten Einwilligungen bereits die grundlegenden gesetzlichen Anforderungen nicht erfüllten.

Bei einer später in 2021 durchgeführten weiteren Untersuchung konnte festgestellt werden, dass viele Anbieter ihre Websites zwischenzeitlich jedenfalls teilweise an datenschutzrechtliche Anforderungen angepasst hatten.

Da die in Aussicht stehende Einführung des TTDSG (vgl. oben 2.1) eine dann unstreitige und jedenfalls in gewisser Weise auch veränderte Rechtslage erwarten ließ und andererseits auch eine Fortentwicklung der von den Datenschutz-Aufsichtsbehörden in Europa vertretenen Auffassungen zu diesem Thema im Rahmen der Taskforce Banner (vgl. oben 1.3) zu erwarten war, wurde seitens des Mediendatenbeauftragten bislang darauf verzichtet, die Untersuchungsergebnisse direkt in Aufsichtsverfahren münden zu lassen. Bei aktuellen Fällen und insbesondere im Rahmen von Beschwerdeverfahren bildeten die oben genannten Problemlagen häufig einen erheblichen Teil der jeweiligen Verfahren, in welchen bilateral zumeist erhebli-

che Verbesserungen erreicht werden konnten. Andererseits war auch in 2021 bereits geplant, die maßgeblichen Erkenntnisse für eine rechtskonforme Ausgestaltung von Webangeboten an die Anbieter im Rahmen von Workshops weiterzugeben. Die entsprechende Workshopreihe wurde im Folgejahr wieder aufgenommen.

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 hiervon kann nicht nur gegenüber dem Verantwortlichen, sondern auch gegenüber Auftragsverarbeitern verhängt werden.

Im Berichtszeitraum hat sich der Medienbeauftragte für den Datenschutz ausgehend von seinem Beratungsauftrag auch weiterhin und im Schwerpunkt darauf konzentriert, soweit es nicht galt, rechtswidrige Verhältnisse umgehend abzustellen, zunächst für ein hinreichendes Verständnis der datenschutzrechtlichen Rechtslage sowie daran anschließend in Zusammenwirkung mit den Verantwortlichen für datenschutzkonforme Lösungen zu sorgen. Konkrete Abhilfebefugnissen standen daher nicht im Zentrum der Tätigkeit – dies insbesondere auch im Hinblick darauf, dass die Mehrzahl der Verantwortlichen, die der Aufsicht des Mediendatenbeauftragten unterliegen, den Regelungen des Medienprivilegs nach Art. 85 DS-GVO (vgl. hierzu näher 3.1.4) unterfallen.

Soweit auf Beschwerden Betroffener hin Datenschutzverstöße im Raum standen, wurden auch in diesem 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 2021 bestehende Mängel abgestellt und so eine datenschutzkonforme Verarbeitung schnell wiederhergestellt

werden. Darüber hinausgehende datenschutzrechtliche Maßnahmen waren hierfür in der Regel nicht erforderlich.

Bei 35 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 überprüfen und in Einzelfällen nachzubessern. Verwarnungen nach Art. 8 Abs. 2 lit. b DS-GVO wurden im Berichtszeitrum nicht ausgesprochen.

Von der Möglichkeit der Verhängung von Geldbußen nach Art. 83 DS-GVO hat der Mediendatenbeauftragte im Berichtszeitraum 2021 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 an.

So veröffentlichte der Mediendatenbeauftragte z. B. im Zuge der Microsoft Exchange Zero-Day Sicherheitslücke (vgl. oben 3.5) auf seiner Website Verhaltenshinweise für betroffene Verantwortliche mit weiterführenden Links und wies in diesem Zusammenhang auf die grundsätzliche Meldepflichtigkeit nach Art. 33 DS-GVO hin.

Regelmäßig steht der Medienbeauftragte für den Datenschutz in engem Austausch mit den Anbietern und berät diese nach Bedarf zu verschiedenen Fragestellungen, wie beispielsweise zur Gestaltung von *Cookie Bannern* auf Homepages, zur Gestaltung von Consent Management Plattformen bei HbbTV oder zum Thema *Consent Tools*.

Ebenfalls führte er eine Informationsveranstaltung zur Einführung in die Grundlagen des Datenschutzes bei der MEDIASCHOOL BAYERN gGmbH, einer Gesellschaft, an der die Landeszentrale als Hauptgesellschafterin beteiligt ist, durch. Grundsätzlich konnte aufgrund der reduzierten Besetzung des Teams des Mediendatenbeauftrag-

ten im Jahr 2021 eigene Veranstaltungen nur in sehr geringem Rahmen umgesetzt werden.

Der Medienbeauftragte für den Datenschutz und sein Team selbst nahmen an verschiedenen juristischen Fortbildungsveranstaltungen, Fachveranstaltungen aus dem Datenschutzbereich und der Datenschutzcommunity, wie beispielsweise den Bayerischen Datenschutztagen, sowie fachübergreifenden Tagungen teil.

Die im Vorjahr begonnene Workshopreihe zur Ausgestaltung von Onlineangeboten war im Berichtsjahr einerseits aus Kapazitätsgründen und andererseits im Hinblick auf die mit der Einführung des TTDSG (vgl. oben 2.1) einhergehenden Rechtsänderungen unterbrochen worden, und wurde erst im Folgejahr wieder aufgenommen.

3.7 Zahlen und Fakten im Überblick

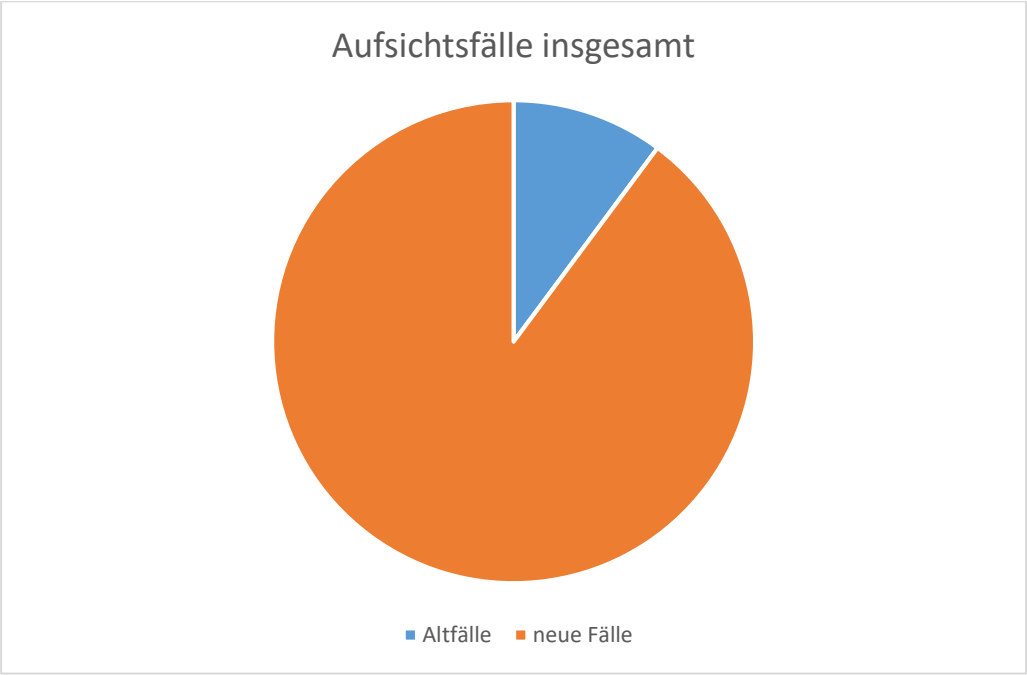
Im Folgenden wird abschließend ein kurzer Überblick über den Umfang der bearbeiteten Fälle und dessen Entwicklung gegeben. Der vorliegende Bericht bezieht sich auf den Zeitraum vom 01.01.2021 bis 31.12.2021.

Im Jahr 2021 blieb zwar einerseits die Anzahl der Beratungen, Beschwerden und gemeldeten Datenschutzverletzungen auf konstant hohem Niveau wie auch im Vorjahr; andererseits differenzierte sich die Gewichtigkeit der einzelnen Beschwerdefälle und der gemeldeten Datenschutzverletzungen. Waren vorher die einzelnen Fälle vergleichbar bedeutsam und zeitintensiv in der Bearbeitung, entwickelten sich in 2021 einige zu thematischen Schwerpunktfällen, die das Team des Medienbeauftragten für den Datenschutz mit einer intensiven iterierenden Bearbeitung über einen längeren Zeitraum in Anspruch nahmen. Schwerpunktthemen waren bei den Beschwerdefällen zunächst der sogenannte „Drittlandstransfer", also die Übermittlung personenbezogener Daten an Empfänger außerhalb der EU. Besonders aber die Gestaltung von *Cookie Bannern* und *Consent Tools* und der Umgang mit sogenannten „Dark Pattern" sowie die Frage nach der datenschutzkonformen Einbindung eingesetzter *Tracking Tools* auf Webseiten rückten immer mehr in den Mittelpunkt der Aufsichtstätigkeit des Mediendatenbeauftragten. Bei den gemeldeten Datenschutzverletzungen nahmen unter anderem Fehlversandfälle weiterhin einen großen Raum ein: Hier wurden jeweils unbefugten Dritten personenbezogene Daten einer betroffenen Person offengelegt. Aus der Analyse derartiger Vorfälle konnten im Rahmen unser Aufsichtstätigkeit Hinweise auf betrügerische Machenschaften eines Dienstleisters bzw. seiner Mitarbeiterinnen und Mitarbeiter herausgearbeitet werden, die zur Aufdeckung eines umfangreichen Falles von Datenmissbrauch führten. Aber auch die Meldungen eines sogenannten „Cyberangriffs" und vier Zero-

Day-Lücken in lokal (on premise) betriebenen Exchange-Servern[40] beschäftigten das Team des Mediendatenbeauftragten intensiv.

Am Ende des vorangegangenen Berichtszeitraumes waren noch insgesamt 18 Verfahren offen und wurden im aktuellen Berichtszeitraum weiter bearbeitet.

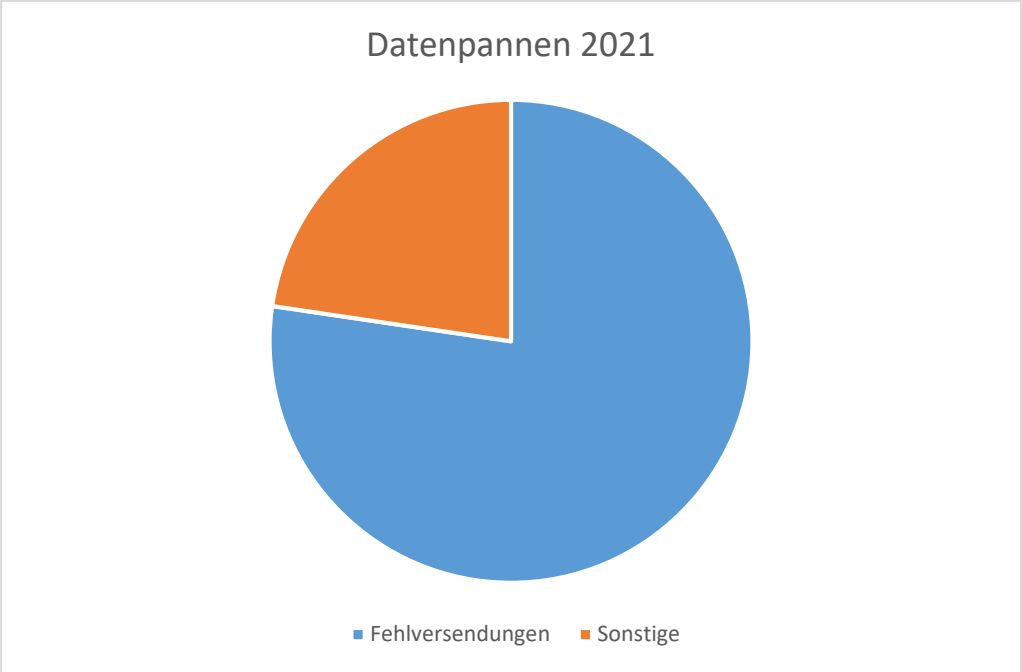
Zu den genannten Verfahren kamen im Jahr 2021 insgesamt 159 neu eingeleitete Verfahren hinzu.



[40] Weitere Informationen unter https://www.blm.de/datenschutzaufsicht/exchange_luecke.cfm (zuletzt abgerufen am 15.09.2022).

Die gemeldeten Datenpannen belaufen sich auf 75 Stück, die Anzahl der Beschwerden und Kontrollanregungen beläuft sich auf 65.

Vorrangig handelte es sich bei den uns gemeldeten Datenpannen leider nach wie vor zum großen Teil (58 Stück) um Fehlversendungen, deren Inhalt von belangloseren Werbemails bis hin zu gesamten Vertragsunterlagen, Bankdaten und vollständigen Datenauskünften alles umfasste. Häufig wird menschliches Versagen als Ursache angegeben. Zumeist lassen sich auch keine anderen Gründe ermitteln. Auffallend war jedoch der Anstieg von Fallgestaltungen, die auf Identitätsdiebstähle hindeuteten. In einigen Fällen ergaben sich bei unseren Nachforschungen Hinweise auf eine mögliche Betrugskonstellation, die jedenfalls auch aufgrund unserer Hinweise aufgedeckt werden konnte. Die daraufhin eingeleiteten Verfahren bis hin zur strafrechtlichen Aufarbeitung dauern noch an.



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.

Auffallend im Jahr 2021 ist die Anzahl von Beschwerden, die sich mit dem Thema Tracking und der Gestaltung von sogenannten Consent Management Bannern beschäftigen, die umfassende technische Sicherungen bei der Aufsicht erfordern und daher sowohl personell als auch zeitlich mit dem vorhandenen Personal nur schwierig zu bearbeiten sind. Dauerthemen sind, wenn auch in der Tendenz eher abnehmend, Datenverarbeitungen trotz Widerrufs und nicht bzw. vorgeblich nicht umgesetzte Löschersuchen; in der Regel waren allerdings die gesetzlich vorgeschriebenen Aufbewahrungsfristen noch nicht abgelaufen, so dass einstweilen nur eine Sperrung erfolgen kann. Die Anzahl der Anfragen, die umfangreich genug waren, dass sie zu aktenkundigen Vorgängen führten, belief sich 2021 auf 19. Hinzu kommen allerdings noch zahlreiche weitere Anfragen, die kurzfristig in Ad-Hoc-Beratungen geklärt werden konnten und nicht eigens gezählt wurden.

3.8 Ausblick

Mit der Geltung der DS-GVO im Mai 2018 stand die Aufsichtspraxis in Deutschland im Allgemeinen und des Medienbeauftragten im Besonderen zunächst ganz im Zei-

chen der neuen Vorgaben, der Anpassung an diese, der Begleitung dieser Anpassungen auf der Ebene der für die jeweiligen Datenverarbeitungsprozesse Verantwortlichen und der Beratung dieser Verantwortlichen in allen damit zusammenhängenden Fragen. Grundsätzlich zeigte sich im Jahr 2021, dass diese Übergangsphase auch im Zuständigkeitsbereich des Mediendatenbeauftragen nun langsam überwunden und in eine routiniertere Aufsichtspraxis mit der Bearbeitung zahlreicher konkreter Aufsichtsfälle übergegangen ist. So kann der Mediendatenbeauftragte seit Mai 2018 auf eine von Jahr zu Jahr steigende Anzahl an eingehenden Beratungsanfragen, Beschwerden zu Datenschutzverletzungen sowie gemeldeten Datenpannen zurückblicken.

So lag auch in diesem Berichtszeitraum der Schwerpunkt der Tätigkeit des Medienbeauftragten bei der Kernaufgabe aller Datenschutzaufsichtsbehörden, nämlich die Einhaltung der Datenschutzvorgaben zu überwachen und diese durchzusetzen[41]. Dabei bilden den Ausgangspunkt in aller Regel Beschwerden und Kontrollanregungen betroffener oder besorgter Bürgerinnen und Bürger: Mit der Einschaltung der Datenschutzaufsicht gelang es in aller Regel, ihre Rechte zu verwirklichen. Hierbei handelt es sich um den Kernbereich des vom Gesetz vorgesehenen Nutzerschutzes, dem daher auch eine entsprechende Aufmerksamkeit gebührt.

Gleichfalls zum Nutzerschutz gehört 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 jedenfalls für die Zukunft sicherstellen soll. Dass der Meldepflicht von Datenpannen und der Behandlung derselben durch die Aufsicht ein darüber hinausgehender Sicherungszweck innewohnt, belegt die in diesem Bereich 2021 zur Aufdeckung gelangte Betrugsreihe.

Daneben bemühen sich der Medienbeauftragte und sein Team nach Kräften, den Anbietern wie auch der Landeszentrale für Beratungen fallspezifisch wie auch abstrakt zur Verfügung zu stehen, was aber voraussetzt, dass das Datenschutzteam auf allen relevanten Themenfeldern auf der Höhe der aktuellen Diskussion und sprachfähig ist, was eine entsprechende Personalausstattung voraussetzt. 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 beitra-

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

gen, künftige datenschutzrechtliche Probleme rechtzeitig zu erkennen und möglichst frühzeitig zu entschärfen oder auch zu lösen.

Seit Herbst 2020 ist der Medienbeauftragte für den Datenschutz in zwei Task Forces (Banner und 101 Beschwerden) auf europäischer Ebene eingebunden, die mit der Nutzung der Angebote von Google und Facebook und dem damit einhergehenden laufenden Datentransfer in die USA einerseits und den Grundlagen für die aktuelle Form der Online-Werbung andererseits in zwei zentralen Datenschutzfragen versuchen, die europäische Datenschutzpraxis für die Zukunft auszugestalten: Dies führte zur zeitlich intensiven Einbindung und Mitarbeit in den Task Forces einerseits und zur stärkeren Zusammenarbeit mit den nationalen und europäischen Datenschutzaufsichten und -institutionen andererseits. Diese Arbeit in den Task Forces und der verstärkte Austausch mit den anderen Behörden wird sich auch in 2022 fortsetzen.

Aufgrund der reduzierten Besetzung des Teams des Medienbeauftragten für den Datenschutz konnten im Jahr 2021 leider keine Anbieterworkshops durchgeführt werden. Zudem verringerten die äußeren Umstände bedingt durch die Corona-Pandemie die Möglichkeiten für persönlichen Kontakt und Austausch und so auch für entsprechende Veranstaltungsformate. An dieser Stelle haben dafür Online-Meetings, telefonischer Austausch und individuelle Beratung einen großen Raum eingenommen.

Für das neue Jahr 2022 sind derzeit drei Anbieterworkshops geplant, die sich vor allem mit den Fragestellungen und Neuerungen der neuen Orientierungshilfe für Anbieter von Telemedien der DSK auseinandersetzen werden. Insofern es die äußeren Umstände erlauben, sollen diese als Hybridveranstaltungen online und in Präsenz in der Landeszentrale umgesetzt werden.

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: Diese soll im kommenden Berichtszeitraum weiter ausgebaut und entsprechende Veranstaltungen angeboten werden.

Zudem werden auch in der folgenden Berichtsperiode Prüfungen und Kontrollmaßnahmen weiter an Bedeutung gewinnen. Diesen 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 In-

formationsveranstaltungen, 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.