



4. Tätigkeitsbericht des Medienbeauftragten für den Datenschutz

bei der Bayerischen Landeszentrale für neue Medien
(Berichtszeitraum: 01.01.–31.12.2022)

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

Datenschutz in Bayern

In Bayern geht man gerne einen eigenen Weg. So liegt – anders als in den meisten anderen Bundesländern – 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 sowie 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 Artikel 51 DS-GVO für das bayerische private Rundfunkmodell geschaffen. Dieser vierte Bericht des Medienbeauftragten für den Datenschutz über das Kalenderjahr 2022 gibt einen Einblick in unsere Aufgaben und Tätigkeitsfelder und stellt zugleich die Schwerpunkte unserer Arbeit in dieser Berichtsperiode heraus. Er gibt zunächst einen Überblick über Positionierung, Behördenstruktur, Aufgaben und Tätigkeitsbereiche des Medienbeauftragten sowie die Zusammenarbeit mit anderen Aufsichtsbehörden, bevor auf die aktuelle gesetzliche Entwicklung in Datenschutzfragen für den Medienbereich eingegangen wird. Daran schließen sich die Überprüfung von Websites, Umsetzungs- und Aufsichtsmaßnahmen und unsere Beratungstätigkeiten und Fortbildungsveranstaltungen an und leiten über zu Zahlen und Fakten zu unseren Tätigkeiten. Diese liefern eine abschließende Zusammenfassung und gehen zum Ausblick ins neue Jahr 2023 über.

Neues TTDSG

Das neue Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), das am 01.12.2021 in Kraft trat, machte sich insbesondere im Jahr 2022 bemerkbar. Nach wie vor war das Urteil des Europäischen Gerichtshofs (EuGH) zum transatlantischen Datenverkehr auf der Grundlage des EU-US Privacy-Shield (Schrems II) und die sich

daraus ergebenden Folgewirkungen relevant, auch wenn sich der Versuch einer neuen politischen Lösung abzeichnete. Auch die vom Europäischen Datenschutzausschuss (EDSA) herausgegebenen Guidelines und die Orientierungshilfen der deutschen Datenschutzkonferenz (DSK) nahmen Einfluss auf die aktuellen Entwicklungen, insbesondere die beiden Aktualisierungen der Orientierungshilfe für Telemedienanbieter zum Jahreswechsel 2021/22 wie auch zum Jahresende 2022.

Europäische Zusammenarbeit in den Task Forces

Weiterhin von großer Bedeutung für unsere Aufsichtstätigkeit 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 Rights¹ gegen Datenschutzverletzungen von (großen) Unternehmen koordiniert zu begegnen und auf europäischer Ebene eine einheitliche Aufsichtspraxis zu gewährleisten.

Vor allem Cookies

Im Jahr 2022 beschäftigten uns im Bereich der Beschwerden und Kontrollanregungen vor allem solche zu den Themen Auskunftsanspruch, Datenlöschung, *Cookie Banner*, *Consent-* und *Tracking Tools*, Werbung trotz Widerrufs sowie Datentransfer in Drittstaaten. Schließlich nahmen die Meldungen der Verletzung des Schutzes personenbezogener Daten, sogenannte Datenpannen, häufig aufgrund von Fehlversendungen und Veränderung von Bankdaten, einen großen Teil unserer Aufsichtstätigkeit ein.

Corona

Auch im dritten Pandemiejahr blieben deren Auswirkungen auf die Arbeitsorganisation des Medienbeauftragten für den Datenschutz und sein Team spürbar. Durch die pandemiebedingte Wechselbelegung der Büroräume erfolgte eine zunehmende Digitalisierung von internen Meetings, aber auch der Austausch mit Stakeholdern und anderen Aufsichtsbehörden erfolgte nach wie vor online. Der im Juli organisierte Anbieterworkshop fand nach verhaltener Anmeldung für die Präsenzveranstaltung zusätzlich online mit reger Beteiligung statt.

¹ Das Akronym noyb leitet sich von folgendem Satz ab: My Privacy is None of Your Business (www.noyb.eu, zuletzt abgerufen am 28.09.2023).

München, 26.09.2023

A handwritten signature in blue ink, appearing to read 'Andreas Gummer', written in a cursive style.

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

Inhalt

Vorbemerkung	- 3 -
Inhalt	- 6 -
1. Der Medienbeauftragte für den Datenschutz und seine Aufgaben.....	- 8 -
1.1 Rechtliche Einordnung als Aufsicht	- 8 -
1.2 Aufgaben und Befugnisse.....	- 9 -
1.3 Zusammenarbeit mit anderen Behörden und Institutionen	- 9 -
2. Interessante Entwicklungen im Fokus	- 13 -
2.1 Wichtige gesetzliche Neuerungen	- 13 -
2.2 Urteile des EuGH zum EU-US Privacy-Shield und des OVG Schleswig-Holstein zu Fanpages: Folgen und Herausforderungen für die Aufsichtspraxis	- 14 -
2.2.1 Internationaler Datenverkehr („Schrems II“) / Standardvertragsklauseln.....	- 14 -
2.2.2 Facebook Fanpages	- 15 -
2.3 Europäische Task Forces	- 17 -
2.3.1 Task Force <i>Banner</i>	- 17 -
2.3.2 Task Force <i>101 Beschwerden</i>	- 18 -
2.4 Guidelines und Orientierungshilfen	- 19 -
3. Unsere Tätigkeiten.....	- 21 -
3.1 Anfragen.....	- 21 -
3.1.1 Recht auf Akteneinsicht.....	- 21 -
3.1.2 Reichweitenmessung	- 22 -
3.1.3 Medienprivileg	- 24 -
3.2 Beschwerden und Kontrollanregungen	- 27 -
3.2.1 Auskunftsanspruch	- 28 -
3.2.2 Datenlöschung.....	- 29 -

3.2.3	Cookie Banner und Consent Tools	- 30 -
3.2.4	Werbung trotz Widerrufs	- 31 -
3.2.5	Datentransfer in Drittstaaten	- 32 -
3.2.6	Tracking Tools.....	- 33 -
3.3	Meldung von „Datenpannen“	- 34 -
3.3.1	Allgemeines zu Meldungen nach Artikel 33 DS-GVO	- 34 -
3.3.2	Fehlversand	- 34 -
3.3.3	Veränderung von Bankdaten.....	- 35 -
3.4	Umsetzungs- und Aufsichtsmaßnahmen	- 35 -
3.5	Beratungstätigkeit und Fortbildungsveranstaltungen	- 36 -
3.6	Zahlen und Fakten im Überblick	- 37 -
3.7	Ausblick.....	- 41 -

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 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 Artikel 11 BayMG liegt, und
- die Anbieter².

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 Artikel 85 DS-GVO, vgl. 3.1.3). 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 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 nur dem Gesetz unterworfen und handelt bei der Erfüllung seiner Aufgaben gemäß Art. 52 Abs. 1 DS-GVO völlig unabhängig, was nach der Rechtsprechung des EuGH nicht nur jede direkte und indirekte Einflussnahme ausschließt, sondern bereits Vorgänge, die den Anschein einer solchen Einflussnahme erwecken. Er unterliegt keiner Rechts- oder Fachaufsicht. Näheres zu seiner Stellung ist den Absätzen 1 bis 10 des Artikel 20 BayMG sowie der von der BLM erlassenen „Satzung über den Medienbeauftragten

² Hier ist in erster Linie der Anbieterbegriff nach dem BayMG gemeint.

für den Datenschutz nach dem Bayerischen Mediengesetz“ vom 23. November 2018 (AMBI 2018, S. 20) zu entnehmen.

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 Artikel 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 Artikel 91 DS-GVO genannten Voraussetzungen spezifische Aufsichtsbehörden für den kirchlichen und religiösen Bereich.

Für die bayerischen Datenschutzaufsichtsbehörden sieht Artikel 21 des Bayerischen Datenschutzgesetzes (BayDSG) vor, dass sie regelmäßig die in Erfüllung ihrer Aufgaben gewonnen Erfahrungen austauschen und sich gegenseitig in ihrer Aufgabewahrnehmung unterstützen. In Erfüllung dieser Vorgabe fanden auch im Jahr 2022 ein reger Austausch vor allem mit dem *Bayerischen Landesamt für Datenschutzaufsicht* zu unterschiedlichsten Aufsichtsfragen, daneben aber auch zunehmend mehr Abstimmungsgespräche mit anderen staatlichen Aufsichten statt.

Zuständigkeitsfragen bereiten im Rundfunkdatenschutz seit jeher 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, so dass der Anbieter mit seiner Antragstellung bei einer Landesmedienanstalt seiner Wahl deren Zuständigkeit begründen konnte, konnte das Sitzlandprinzip insoweit nicht zur Anwendung kommen. Mit dem Übergang zum Medienstaatsvertrag (MStV) Ende 2020 hat sich der Gesetzgeber nun auch beim Rundfunk für die Anwendung des Sitzlandprinzips entschieden,³ für zu diesem Zeitpunkt 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 besondere Schwierigkeiten. In der Praxis führte dies dazu, dass Zuständigkeitsfragen für den Bürger im Grenzgebiet zum Rundfunkdatenschutz kaum und auch ansonsten nur schwierig zu durchschauen sind, so dass der Kompetenz des Medienbeauftragten für den Datenschutz in beiden Rechtsgebieten insoweit eine besondere Bedeutung zukommt.

Neben dem gesetzlich durch Artikel 21 BayDSG vorgesehenen Erfahrungsaustausch mit den bayerischen Aufsichtsbehörden nahm der Mediendatenbeauftragte und seine Mitarbeiterinnen und Mitarbeiter⁵ im Berichtsjahr auch an unterschiedlichen Terminen zum Erfahrungsaustausch mit anderen (Datenschutz-)Aufsichtsbehörden teil: Zentral sind vor allem die beiden Sitzungen des Arbeitskreises Medien (AK Medien) der DSK, die in der Regel im Februar und im September des jeweiligen Jahres stattfinden. Daneben war eine mehr oder minder monatlich Abstimmungsrunde mit mediennahen Kollegen der staatlichen Aufsichtsbehörden von besonderer Bedeutung, um aktuellen Aufsichtsentwicklungen folgen zu können. Hinzu kam die Beteiligung des Mediendatenbeauftragten am institutionalisierten Austausch der DSK mit den spezifischen Aufsichtsbehörden⁶, der üblicherweise zweimal jährlich stattfindet.

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.

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 ab. Dies erfolgte insbesondere bei Beschwerdewellen⁷ zu den Themenbereichen Drittlandtransfer und Dark Pattern⁸ ⁹ sowie zum Einsatz von *Tracking Tools*.

Im Hinblick auf die europaweit eingelegten 101 Beschwerden¹⁰ des österreichischen Vereins noyb zum Einsatz von *Google Analytics* und/oder *Facebook Connect* bei größeren Webseitenanbietern fand mit den anderen betroffenen Behörden auch im Jahr 2022 ein regelmäßiger Austausch über das weitere Vorgehen und die erforderlichen rechtlichen Bewertungen statt. Wie in den letzten beiden Berichten bereits erwähnt, wurde beim Europäischen Datenschutzausschuss (EDSA) 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 hatte der Verein noyb im Jahr 2021 eine weitere Beschwerdewelle initiiert: 422 Beschwerden zum Themenkomplex Dark Pattern wurden verteilt über diverse europäische Datenschutzaufsichtsbehörden eingereicht. Der Mediendatenbeauftragte hatte damals fünf dieser Beschwerden in seinem Zuständigkeitsbereich erhalten.

Zur Erlangung einer abgestimmten Vorgehensweise war beim EDSA auch eine Task Force („Banner“) eingerichtet worden, an der der Medienbeauftragte für den Datenschutz auch im Jahr 2022 stets durch eine Mitarbeiterin vertreten war (vgl. hierzu ausführlicher unter 2.3). Begleitend fanden hierzu inhaltliche Abstimmungen unter deutschen Aufsichtsbehörden statt

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.

Darüber hinaus nahm der Mediendatenbeauftragte im Mai 2022 durch eine Mitarbeiterin an einem Online-Treffen der „Cooperation among Consumer and Data Protection Authorities“ teil, einer Gruppe von Freiwilligen aus verschiedenen Mitgliedsstaaten von Verbraucherschutzbehörden (CPC) und Datenschutzaufsichtsbehörden (DPA) sowie der Europäischen Kommission. In dem Treffen wurden eine Reihe von Studien, Guidelines und aktuelle Fälle in Kurzpräsentationen von verschiedenen Vertretern der Behörden dargestellt.

Im Berichtszeitraum war erwogen worden, ob eine Klarstellung der Zuständigkeiten für unterschiedliche Vorgaben des TTDSG möglicherweise sinnvoll erscheinen könnten. Da sich hieraus auch Anpassungsbedarf für das BayMG ergeben könnte, hatte der Medienbeauftragte auch in 2022 zu diesem Thema eine Stellungnahme abgegeben und auf einen aus seiner Sicht bestehenden Änderungsbedarf hingewiesen. Das betreffende Gesetzgebungsverfahren ist bisher noch nicht abgeschlossen.

2. Interessante Entwicklungen im Fokus

2.1 Wichtige gesetzliche Neuerungen

Eine ePrivacy-Verordnung gibt es nach wie vor nicht, so dass die ePrivacy-Richtlinie aus dem Jahr 2002¹¹ mit ihrer Aktualisierung aus dem Jahr 2009 weiterhin gilt. Eine wirkliche Umsetzung in deutsches Recht erfolgte erst zum 1. Dezember 2021 mit dem „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), so dass im Berichtszeitraum erste Erfahrungen in der Anwendung dieses Gesetzes gesammelt werden konnten.

Auf EU-Ebene hat sich aber an anderer Stelle einiges getan: Die im Jahr 2020 von der EU-Kommission angekündigte Digitalstrategie mit einem ganzen Bündel an gesetzlichen Maßnahmen nahm im Berichtszeitraum weiter Gestalt an: Am 24. Juni 2022 trat der *Data Governance Act* (DGA) in Kraft, der mit dem Konzept des Datenaltruismus die Verfügbarkeit von Daten fördern, Mechanismen für die gemeinsame Datennutzung in der EU etablieren und zugleich dem Ziel dienen soll, Vertrauen in die datenvermittelnden Akteure zu schaffen. Am 1. November 2022 ist der *Digital Markets Act* (DMA) in Kraft getreten mit der Zielsetzung, digitale Monopole von marktbeherrschenden Digitalkonzernen (sogenannten „Gatekeepern“) zu bekämpfen und in digitalen Märkten einen fairen Wettbewerb durch gesetzliche Regulierung zu gewährleisten. Der *Digital Services Act* (DSA) trat dann zum 16. November 2022 in Kraft mit der Verpflichtung für große Online-Plattformen zu verbindlichen Verhaltensvorschriften im Kampf gegen rechtswidrige Inhalte, Online-Desinformation oder andere gesellschaftliche Risiken.

All diesen neuen EU-Verordnungen ist nach deren gesetzgeberischer Zielsetzung gemein, dass durch sie die existierenden Vorschriften der DS-GVO „unberührt“ bleiben sollen, beziehungsweise dass sie „unbeschadet“ der DS-GVO gelten sollen. Was das nun im Einzelfall konkret zu bedeuten hat (z. B. im Hinblick auf kollidierende Verhaltensvorschriften, aber auch im Hinblick auf bestimmte möglicherweise divergierende Aufsichtszuständigkeiten), ist entgegen des suggerierten Vorrangs der DS-GVO derzeit noch völlig unklar und seitdem Gegenstand heftiger Diskussionen.

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).

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 wirkte das sogenannte Schrems II-Urteil des EuGH¹² nach, in dem sich das Gericht zum zweiten Mal zur Frage geäußert hat, unter welchen Voraussetzungen ein Datentransfer aus dem europäischen Rechtsraum in die USA zulässig ist.

Der das Privacy Shield betreffende Durchführungsbeschluss der EU-Kommission¹³ wurde in dem oben genannten Urteil vom 16.07.2020 abermals aus Anlass eines Verfahrens der irischen Datenschutzaufsichtsbehörde (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 insbesondere von Grundrechtspositionen von EU-Bürgern 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. Insofern hebt der EuGH hervor, dass der Datenexporteur und der Empfänger der Übermittlung vorab prüfen müssen, ob das erforderliche Schutzniveau so in dem betref-

¹² Urteil des EuGH vom 16. Juli 2020 (Rechtssache C 311/18 – „Schrems II“).

¹³ Durchführungsbeschluss (EU) 2016/1250.

fenden 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 genau zu überprüfen, wobei sich stets die Schwierigkeit ergeben wird, wie im Falle eines amerikanischen Recht entsprechenden Zugriffs gewährleistet werden soll, ein Schutzniveau für den betroffenen EU-Bürger sicherzustellen, welches das amerikanische Recht nicht vorsieht.

Gleichwohl hat der europäische Datenschutzausschuss am 10.11.2020 Empfehlungen beschlossen, die Maßnahmen zur Gewährleistung eines entsprechenden Schutzniveaus darstellen, sogenannte *supplementary measures*, die am 18.06.2021 nochmals angepasst wurden.¹⁴

Ferner hat die Europäische Kommission mit Durchführungsbeschluss 2021/914 vom 4. Juni 2021 neue Standardvertragsklauseln erlassen und am 07.06.2021 veröffentlicht¹⁵. Die neuen Standardvertragsklauseln¹⁶ sind modular aufgebaut und befassen sich mit Übermittlungen von personenbezogenen Daten in Drittstaaten, also Staaten außerhalb des Europäischen Wirtschaftsraumes.

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

2.2.2 Facebook Fanpages

Weiterhin virulent war das Thema der Nutzung von Social-Media-Kanälen und dabei vor allem von Facebook-Fanpages, insbesondere durch öffentliche Stellen. Ein maßgeblicher Ausgangspunkt der Diskussion war die seinerzeitige Anordnung des *Unabhängigen Landeszentrum für Datenschutz* (ULD), nach der die *Wirtschaftsakademie*

¹⁴ 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](https://edpb.europa.eu/our-work-and-activities/our-policies/recommendations/recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf) (europa.eu) (zuletzt abgerufen am 28.9.2023).

¹⁵ Amtsblatt EU L 199/37.

¹⁶ Diese differenzieren zwischen Übermittlungen von Verantwortlichen an Verantwortliche, von Verantwortlichen an Auftragsverarbeiter, von Auftragsverarbeitern an Auftragsverarbeiter und von Auftragsverarbeitern an Verantwortliche.

Schleswig-Holstein GmbH (Wirtschaftsakademie) ihre Facebook-Fanpage wegen Verstößen von Facebook abschalten sollte. Der sich anschließende Rechtsstreit erreichte das Bundesverwaltungsgericht (BVerwG), das zunächst einen Fragenkatalog zur Verantwortlichkeit von Fanpagebetreibern und zur Anwendbarkeit des deutschen Datenschutzrechts dem Europäischen Gerichtshof vorlegte. Der stellte für die üblicherweise anzutreffenden Fallgestaltungen eine weitgehende gemeinsame Verantwortung des Fanpagebetreibers zusammen mit Facebook fest¹⁷. Im Anschluss hob das BVerwG die Entscheidung des OVG Schleswig-Holstein auf und verwies den Streit an das OVG zurück. Das OVG hat daraufhin mit Urteil vom 25.11.2021 einen schwerwiegenden Datenschutzverstoß in der Verwendung der personenbezogenen Daten von Facebook-Nutzern festgestellt. Das maßgebliche Problem bildet dabei die Verknüpfung der Daten von Facebook mit den Daten des Fanpageaufrufs, wenn diese in Profilen gespeichert und zu Werbezwecken genutzt werden und hierfür keine hinreichende Einwilligung der betroffenen Person vorliegt.

Die Verantwortung des Fanpagebetreibers ist danach im Einklang mit der Rechtsprechung des EuGH eine gemeinsame, was nicht zwingend eine gleichwertige Verantwortung bedeutet. Auch wenn sich diese Verantwortung des Fanpagebetreibers nicht auf vor- oder nachgelagerte Vorgänge der Verarbeitungskette bei Facebook erstreckt, betrifft sie jedenfalls neben der Auswertung der Daten aus den jeweiligen Fanpagebesuchen auch die Verwendung der Registrierungsdaten und der übrigen vorhandenen Daten von im jeweiligen Netzwerk registrierten und angemeldeten Personen zur Erstellung der vereinbarten Statistiken (Rn. 154). Der Beitrag des Fanpagebetreibers besteht dabei darin, dass er durch die Einrichtung der Fanpage Facebook die entsprechende Datenverarbeitung ermöglicht, die ohne diese Einrichtung nicht erfolgen würde (Rn. 150).

Diese Rechtsprechung hat ihren Niederschlag in der Aufsichtstätigkeit verschiedener Landesbeauftragter wie auch des Bundesbeauftragten für den Datenschutz gefunden, bei der auch die Vorbildfunktion, die öffentlichen Stellen zukomme, eine Rolle spielte. Sich daraus ergebende Aufsichtsmaßnahmen sind unterdessen Gegenstand gerichtlicher Verfahren.

¹⁷ EuGH, Urteil vom 05.06.2018 – C 210/16.

2.3 Europäische Task Forces

Der Austausch des Mediendatenbeauftragten mit anderen Datenschutzaufsichten zu den Themen Drittlandtransfer und Dark Pattern¹⁸ ¹⁹ sowie zum Einsatz von *Tracking Tools* wurde im Berichtszeitraum in konkreten Aufsichtsfällen und insbesondere Beschwerdewellen²⁰ länder- und behördenübergreifend sowie mit Behörden anderer Mitgliedsstaaten fortgesetzt. Um eine einheitliche Vorgehensweise und Rechtsanwendung auch auf europäischer Ebene zu gewährleisten und eine abgestimmte Vorgehensweise zu erlangen, wurden Task Forces auf europäischer Ebene gegründet.

2.3.1 Task Force *Banner*

Im Jahr 2021 hat der Verein noyb eine Beschwerdewelle bezüglich des Einsatzes von *Cookie Bannern* 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. 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 auch 3.2.3). Begleitend zu diesen Vorgängen fanden laufend inhaltliche Beratungen unter den beteiligten deutschen Aufsichtsbehörden zu den jeweils anstehenden Themen statt,

Die fünf Beschwerden, die in den Zuständigkeitsbereich des Medienbeauftragten für den Datenschutz fallen, 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

¹⁸ 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.

¹⁹ 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.

²⁰ 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.

von *Cookie Bannern*. Die maßgebliche Frage ist, ob die Gestaltung dieser Banner, die Nutzer letztlich rechtswidrig dazu bringen, umfassende Einwilligungen in die Verarbeitung ihrer Daten zu erteilen, ohne dass die Nutzer dies tatsächlich wollen (sogenannte „Dark Pattern“). Die Frage, in welcher Form der Widerruf einer so erteilten Einwilligung ermöglicht werden muss, spielt dabei eine ebenso große Rolle.

Mit den Verantwortlichen befindet sich der Mediendatenbeauftragte noch in laufenden Verwaltungsverfahren. Dabei ist jedoch sehr zu begrüßen, dass seit dem Einleiten der Prüfverfahren inzwischen einige der vorgeworfenen Verstöße durch die Verantwortlichen beseitigt wurden.

Zum Ende des Berichtszeitraumes dauerten die Abstimmungen zu den einzelnen Verstoß-Vorwürfen innerhalb der Task Force noch an, kamen aber Anfang 2023 zu einem gewissen Abschluss (vgl. hierzu unten 3.7).

2.3.2 Task Force 101 Beschwerden

Im Hinblick auf die europaweit öffentlichkeitswirksam eingelegten 101 Beschwerden²¹ des österreichischen Vereins noyb²² zum Einsatz von *Google Analytics* und/oder „Facebook Connect“ bei größeren Webseitenanbietern fand mit den anderen betroffenen Behörden weiterhin ein regelmäßiger Austausch in der vom EDSA gebildeten Task Force „101 complaints“ über das weitere Vorgehen statt. An den Sitzungen der Task Force beteiligte sich eine Mitarbeiterin des Medienbeauftragten für den Datenschutz regelmäßig (vgl. hierzu ausführlicher unter 3.2.5).

Diese 101 Beschwerden wurden gegen in der EU/EWR ansässige Unternehmen eingelegt, die 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)²³ personenbezogene Daten an *Google* bzw. *Facebook* übermitteln, ohne in der Lage zu sein, ein angemessenes Schutzniveau für die personenbezogenen Daten der Beschwerdeführer zu gewährleisten.

²¹ Das Gemeinsame der Beschwerden liegt in den Datentransfers ins nichteuropäische Ausland, die durch bestimmte in die angesprochenen Datenverarbeitungsprozesse eingebundene Tools ausgelöst werden.

²² Noyb – my data is none of your business – ist der vom Datenschutzaktivisten Max Schrems gegründete Verein, der sich insbesondere für von Datenschutzverletzungen Betroffene einsetzt, für diese stellvertretend Klage einreicht und so bereits mehrere Beschwerdewellen losgetreten hat. Weitere Informationen zu noyb auf deren Website unter <https://noyb.eu/de> (zuletzt abgerufen am 08.08.2023).

²³ EuGH Urteil vom 16.07.2020, C-311/18- Schrems II <http://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=DE> (zuletzt abgerufen am 08.09.2023).

Im Jahr 2022 rückten die mit den eingesetzten Facebook Tools verbundenen Problemlagen stärker in den Mittelpunkt. Es folgten Austauschgespräch auf den unterschiedlichsten Ebenen, die auch erstmals etwas genauere Einblicke in die fraglichen Datenverarbeitungsprozesse ermöglichten, auch wenn ein maßgeblich Beteiligter weiterhin den direkten Austausch mit anderen Aufsichtsinstanzen als der für seine Hauptniederlassung zuständigen nationalen Instanz weitgehend ablehnt. Das bei uns anhängige Verfahren berührt wegen der Einbindung des eingesetzten Facebook Tools und der damit einhergehenden Datentransfers, die letztlich wohl in den USA enden, so viele grundlegende Fragen, dass das Verfahren im Berichtszeitraum nicht abgeschlossen werden konnte.

Zum Ende des Berichtszeitraums zeichnete sich auch bei der Task Force „101 complaints“ ab, dass diese im Jahr 2023 zur Veröffentlichung eines Berichts werden können (siehe hierzu auch 3.7).

2.4 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:

- 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 (2. Version vom 14.12.2021)
- Guidelines 01/2022 on data subject rights - Right of access (Version 1.0.vom 18.01.2022)
- Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them
- Guidelines 04/2021 on Codes of Conduct as tools for transfers
- Guidelines 02/2022 on the application of Article 60 GDPR
- Guidelines 04/2022 on the calculation of administrative fines under the GDPR
- Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement
- Guidelines 06/2022 on the practical implementation of amicable settlements
- Guidelines 07/2022 on certification as a tool for transfers

- Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority
- Guidelines 9/2022 on personal data breach notification under GDPR
- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Artikel 47 GDPR)
- Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them
- 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

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)
- Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)
- FAQ zu Facebook-Fanpages
- Auswertungsbericht des AK Medien – Konsultation zur OH Telemedien
- Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021) Version 1.1 vom Dez. 2022

3. Unsere Tätigkeiten

Die praktische Aufsichtstätigkeit ist bei der gegenwärtigen Personalausstattung noch 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 Datenschutzvorfällen, den sogenannten Datenpannen. Im Folgenden werden die dabei im Berichtszeitraum berührten maßgeblichen Fragenkreise dargestellt.

3.1 Anfragen

In diesem Berichtszeitraum verlagerte sich der Schwerpunkt unserer Aufsichtsfälle. Die im folgenden dargestellten Schwerpunkte bei den Anfragen zeigen die inhaltliche Entwicklung in diesem Bereich. Weiterhin ist bemerkenswert, dass sich die Anzahl der Anfragen im Vergleich zum Vorjahr mehr als verdoppelt hat (dazu ausführlich in Kapitel 3.6).

3.1.1 Recht auf Akteneinsicht

Das Recht auf Akteneinsicht folgt in Verwaltungsverfahren dem Prinzip der beschränkten Aktenöffentlichkeit²⁴. Für die betroffenen Parteien eines Verwaltungsverfahrens ergeben sich dennoch in der Regel Einsichtsrechte in die sie betreffenden Akten schon aus rechtsstaatlichen Grundsätzen, allerdings jeweils nach Maßgabe der für das jeweilige Verfahren geltenden gesetzlichen Vorgaben.

Dieses Recht der Parteien eines Verwaltungsverfahrens ist prinzipiell einerseits zu unterscheiden von allgemeinen Auskunftsrechten, die sich aus Informationsfreiheitsgesetzen oder in Bayern aus dem allgemeinen Auskunftsrecht nach Artikel 39 BayDSG ergeben, wie auch andererseits vom Auskunftsrecht nach Artikel 15 DS-GVO. Letzteres räumt allgemein einer Person das Recht ein, von einem datenschutzrechtlich Verantwortlichen Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten und Informationen zu erlangen.

Im Hinblick auf das in Artikel 77 DS-GVO vorgesehene Beschwerderecht hat der bayerische Gesetzgeber mit Art. 20 Abs. 2 BayDSG eine Vorschrift erlassen, die sich nur auf dieses spezielle Verfahren bezieht und hierzu eine gesetzliche Sonderrege-

²⁴ Vgl. Stelkens/Bonk/Sachs, Kommentar zum Verwaltungsverfahrensgesetz § 29 Rn. 1.

lung schafft. Diese nimmt einerseits die besondere Situation eines datenschutzrechtlichen Beschwerdeverfahrens, andererseits aber auch die in einem solchen Verfahren geltenden Rahmenbedingungen einschließlich der dabei zu berücksichtigenden Vertraulichkeitsinteressen in den Blick.

Der bayerische Gesetzgeber hat unter Berücksichtigung und Abwägung dieser Interessen für diese Verfahren die gesetzliche Anordnung getroffen, dass Auskunfts- oder Einsichtsrechte hinsichtlich Akten und Dateien der Datenschutzaufsichtsbehörden bei derartigen Beschwerdeverfahren nicht bestehen. Die Vorschrift unterstreicht damit die besondere Zweckbindung der in Wahrnehmung der datenschutzrechtlichen Überwachungsaufgaben gewonnenen Informationen²⁵. Diese stammen einerseits vom Beschwerdeführer, der je nach Fallgestaltung unterschiedlichste Interessen an der Geheimhaltung der ihn betreffenden Informationen haben kann, aber gegenüber der Aufsichtsbehörde prinzipiell auch nur die Rechte aus Artikel 78 DS-GVO hat. Andererseits ist die Aufsichtsbehörde in Wahrnehmung ihrer unabhängigen Kontrollaufgabe auch auf Auskünfte des Verantwortlichen angewiesen, den insoweit Mitwirkungs- und Auskunftspflichten treffen.

Für diese sehr speziell zugeschnittene Situation hat sich der Gesetzgeber unter Abwägung der verschiedenen, die unterschiedlichen Rechte der betroffenen Parteien berührenden Interessen dafür entschieden, keine Auskunfts- oder Einsichtsrechte in die Akten und Dateien der jeweiligen Datenschutzaufsichtsbehörde zuzulassen, um den Besonderheiten des Beschwerdeverfahrens gerecht zu werden, aber auch um der jeweiligen Aufsichtsbehörde die in diesem Verfahren steckenden Möglichkeiten, für rechtmäßige Verhältnisse zu sorgen, möglichst weitgehend zu erhalten. Gleichwohl ist die so geregelte Situation Gegenstand zahlreicher Erörterungen in entsprechenden Verfahrenssituationen sowohl mit Beschwerdeführern wie auch Verantwortlichen.

3.1.2 Reichweitenmessung

Der Einsatz von Tools zur Reichweitenmessung auf Websites – häufig in Verbindung mit der Implementierung von Consent-Management-Plattformen (CMP, vgl. hierzu näher 3.2.3) – war ein Themenkomplex, der im Berichtszeitraum an den Mediendatenbeauftragten wiederholt herangetragen wurde, so dass sich dieser hiermit vertieft auseinandergesetzt hat.

²⁵ Vgl. HK-BayDSG/Kai Engelbrecht BayDSG Art. 20 Rn. 20.

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 (z. B. Matomo On-Premise), die unter Umständen auch nach dem Prinzip *data protection by design/default* konfiguriert werden können, und der Anbieter auch keine individuellen Nutzerprofile erstellt, 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 gemäß Art. 6 Abs. 1 lit. f DS-GVO rechtfertigen, so dass nicht unbedingt eine Einwilligung, sondern lediglich die Möglichkeit eines Widerspruchs erforderlich wäre. Allerdings steht dem der § 25 TTDSG häufig entgegen, welcher die Vorschrift des Art. 5 Abs. 3 ePrivacy-Richtlinie (RL 2002/58/EG) ins nationale Recht umgesetzt hat; nach Artikel 95 DS-GVO hat die ePrivacy-Richtlinie (bzw. das nationale Umsetzungsgesetz) Vorrang gegenüber der DS-GVO und verdrängt die dort enthaltenen Rechtsgrundlagen. Nach § 25 Abs. 1 TTDSG ist das Speichern von oder der Zugriff auf Informationen auf dem Endgerät des Nutzers (z. B. Cookies) nur zulässig, wenn der Nutzer eingewilligt hat. Einer Einwilligung bedarf es nach § 25 Abs. 2 TTDSG lediglich dann nicht, wenn der alleinige Zweck der Speicherung von Informationen oder des Zugriffs auf bereits gespeicherte Informationen die Durchführung der Übertragung einer Nachricht ist (vgl. Nr. 1) oder die Speicherung von Informationen oder der Zugriff auf bereits gespeicherte Informationen unbedingt erforderlich ist, damit ein vom Nutzer ausdrücklich gewünschtes Angebot vom Anbieter zur Verfügung gestellt werden kann (vgl. Nr. 2).

Da die Voraussetzungen dieser Ausnahmebestimmung in der Regel nicht erfüllt werden, ist eine einwilligungsfreie Reichweitenmessung zumeist nur dann auf rechtlich zulässige Art und Weise implementierbar, wenn auf dem Endgerät des Nutzers weder Informationen gespeichert werden, noch auf Informationen (aktiv) zugegriffen wird. Der Einsatz von JavaScript zur Reichweitenmessung dürfte folglich ohne eine Einwilligung des Nutzers in der Regel unzulässig sein und so erst dann auf dem Endgerät des Nutzers geladen werden, nachdem dieser seine Einwilligung hierzu erteilt hat. Dasselbe gilt für den Einsatz von sogenannten *Tracking Pixel* oder *Web Beacons*. Bei all diesen Technologien findet ein aktives Speichern von Informationen auf dem Endgerät des Nutzers statt, welche dann im Anschluss aktiv Informationen zurück an den Anbieter schicken.

Bei der Frage nach der Zulässigkeit kommt es auf den Einsatz von Cookies nicht an. Auch ein sogenanntes *cookie-less tracking* muss die Vorschriften des § 25 TTDSG beachten; wenn für die Reichweitenmessung ein JavaScript genutzt wird und dieses auf

dem Endgerät geladen wird, bevor der Nutzer seine Einwilligung hierzu erteilt hat, ist auch dieses *cookie-less tracking* unzulässig.

Wenn hingegen eine Reichweitenmessung implementiert wird, die tatsächlich ohne ein Speichern von bzw. ohne Zugriff auf Informationen auf dem Endgerät auskommt, dürfte dies zumindest ohne Einwilligung nach § 25 TTDSG möglich sein.

Soll ausnahmsweise die Reichweitenmessungen als unerlässlicher Teil des vom Nutzer ausdrücklich gewünschten Telemediendienstes zulässig sein, weist die OH Telemedien 2021 zu Recht darauf hin, dass hierfür hohe Hürden bestehen, die in solchen Fällen erfüllt sein müssen.

3.1.3 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 verfassungs- und europarechtlich 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. Seither sind die Regelungen der DS-GVO verbindlich anzuwenden, so dass 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 jeweils individuell Betroffenen zu genügen und deren Rechte zu gewährleisten hat. Zudem unterliegt er bei Verstößen gegen diese Regeln erheblichen Haftungsverpflichtungen sowie 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 dem Recht auf freie Meinungsäußerung und damit 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 mit § 12 MStV²⁶ einen sehr weitgehenden Gebrauch gemacht²⁷.

Dies führt dazu, dass es für die Verarbeitung personenbezogener Daten zu journalistischen Zwecken jenseits dieser Zwecksetzung keiner weiteren Rechtsgrundlage bedarf, bei der journalistischen Tätigkeit lediglich das in § 12 MStV niedergelegte Datengeheimnis zu beachten ist 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 auf sie bezogenen Daten gespeichert sind, nur den 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 maßgeblich 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 an ihn in diesem Zusammenhang immer wieder Fragen von ganz grundlegender bis hin zu sehr spezieller Gestaltungen herangetragen.

²⁶ Unter Geltung des RStV war dies der dortige § 9c.

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 Artikel 11 BayPrG und im Übrigen Artikel 38 BayDSG zu erwähnen.

Neben Anwendungsfolgen im Detail steht vor allem die Frage im Zentrum, wer sich auf das Medienprivileg berufen kann, wofür es letztlich darauf ankommt, welche Ausgestaltung der Gesetzgeber dem Begriff der journalistischen Zwecke geben 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 Rundfunkprogramme²⁸ und damit auch zahlreiche Angebotsformen des Internets mit in den Blick nimmt. Andererseits hatte der EuGH in einem grundlegenden Urteil²⁹ festgestellt, dass der Begriff des Journalismus in Anbetracht der Bedeutung, die der Freiheit der Meinungsäußerung in jeder demokratischen Gesellschaft zukomme, weit auszulegen sei und der Begriff der journalistischen Tätigkeiten daher nicht auf Berufsjournalisten beschränkt werden dürfe. Vielmehr komme es darauf an, ob bei einer Äußerung der Zweck im Vordergrund stehe, Informationen, Meinungen und Ideen in der Öffentlichkeit zu verbreiten. Auf eine bestimmte Form der Verbreitung kommt es daher nicht an. Das Internet als Verbreitungsmedium ist ausreichend.

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 Dennoch werden von der Rechtsprechung nicht alle redaktionell gestalteten Angebote als journalistisch anerkannt. Vielmehr müssten neben der Absicht der Berichterstattung auch Tätigkeiten vorliegen, die der Erfüllung der Aufgaben einer funktional verstandenen Presse bzw. des Rundfunks dienen.³¹

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.³² Ob dies bei der gegenwärtigen deutschen Rechtslage hinreichend geschehen sei, ist unter den deutschen Aufsichtsbehörden durchaus strittig wie auch

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.

²⁹ Urteil des EuGH vom 14.2.2019 - C-345/17, Rn.51 ff.

³⁰ Vgl. Begründung zu § 2 MStV.

³¹ Beschluss des OLG Koblenz vom 12.4.2021 – 4 W 108/21.

³² Urteil des EuGH vom 14.2.2019 - C-345/17, Rn.63 ff.

die Frage, ob die deutsche Rechtslage wegen des Anwendungsvorranges des Europarechts gegebenenfalls ignoriert werden dürfte.

Inhaltliche Bedeutung erlangen Fragen nach dem Medienprivileg häufig bei journalistischen Aussagen, die das Persönlichkeitsrecht der dargestellten Personen bzw. derjenigen, über welche berichtet wird, zu tangieren geeignet sind. In diesen Fallgestaltungen ergeben sich daher häufig gewisse Parallelitäten zu Fragen des Persönlichkeitsrechtes bzw. der zu beachtenden journalistischen Grundsätze. Da das Persönlichkeitsrecht mehr als das Rundfunkrecht auf eine reichhaltige Kasuistik und eine langjährige Rechtsprechungstradition verweisen kann, sind dem Persönlichkeitsrecht häufig maßgebliche Weichenstellungen inhaltlicher Natur zu entnehmen.

In der Praxis des Mediendatenbeauftragten erlangt unterdessen aber auch die Kehrseite des Medienprivilegs, das Datengeheimnis, eine 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 Zwecken untersagt und für Zuwiderhandlungen sogar erhebliche Sanktionen vorsieht. In der Praxis bedeutet dies, dass mit der Aufnahme einer journalistischen Tätigkeit zu einem bestimmten Sachverhalt die dabei verwendeten und gesammelten Informationen dem oben genannten Datengeheimnis unterliegen. Den mit dieser journalistischen Tätigkeit befassten Personen wird ab diesem Zeitpunkt eine sehr weitgehende Geheimhaltungsverpflichtung für alle anderen Zwecke auferlegt, so dass eine Verwendung dieser Daten in nahezu allen anderen Zusammenhängen unterbleiben muss.

3.2 Beschwerden und Kontrollanregungen

Die Anzahl der Beschwerden und Kontrollanregungen ist mit insgesamt 74 im Jahr 2022 neu eingereichten Eingaben weiterhin hoch. Es erreichten den Mediendatenbeauftragten – zum Teil ins Detail gehende – Fragen und Eingaben zu unterschiedlichen Themen, wobei solchen zu Cookies und Trackern auf Websites sowie Fragen zur Zulässigkeit von unterschiedlichsten Formulierungen in Datenschutzerklärungen und der Gestaltung von CMPs eine besondere Bedeutung zukam. Dies belegt nachdrücklich, dass das Interesse der Bevölkerung an Datenschutzfragen unvermindert hoch ist.

Vereinzelt erreichten den Mediendatenbeauftragten auch Eingaben von Bürgern, die ein gewisses Vorwissen haben, was die Bearbeitung erleichtert. Gelegentlich bestehen aber auch falsche oder vermeintliche Kenntnisse in rechtlicher Hinsicht. Dies kann

die Kommunikation mit dem jeweiligen Petenten dann mitunter sehr erschweren. Daher ist es unausweichlich, bei den Bürgern die Sensibilität im Bereich des Datenschutzes weiterhin aufrecht zu erhalten, aber auch die zum Teil bereits vorhandenen Kenntnisse zu erweitern und gelegentlich bestehende Fehlvorstellungen auszuräumen.

Technische Sachverhalte werden verstärkt in den Fokus gerückt, 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.

Das zum Ende des Berichtsjahres 2021 aufgetretene Phänomen, dass vermehrt „Musterbeschwerden“ oder gar „Beschwerdegeneratoren“ genutzt wurden, die automatisiert eine Vielzahl von gleichartig gelagerten Beschwerden gegen unterschiedliche Verantwortliche in kurzer Zeit produzieren, setzte sich im ersten Quartal 2022 fort und ebte dann schlagartig ab. Problematisch an diesen Fällen war, dass die Beschwerdeführer mittels vorgenerierter Textbausteine ausführlich eine Vielzahl von Datenschutzverletzungen (zumeist Einsatz von Tracking-Tools ohne die erforderliche Nutzereinstimmung) auf Webseiten behaupteten und mittels undatierter Screenshots zu belegen schienen, die bei einer technischen Überprüfung aber letztlich gar nicht festzustellen waren. Nachfragen unsererseits bei den Betroffenen führten oftmals ins Leere bzw. erschöpften sich in einer Wiederholung des Beschwerdevortrags. Dies führte auf Aufsichtsseite auch weiterhin zu erheblichen Belastungen und letztlich Kapazitätsengpässen, da derartige automatisierte Prozessabläufe bei der Beschwerdebearbeitung beim Medienbeauftragten für den Datenschutz nicht möglich sind. Jeder Fall muss individuell behandelt und beantwortet werden, solange er als individuelle Beschwerde eingereicht wird.

3.2.1 Auskunftsanspruch

Auch im Berichtsjahr 2022 befasste sich ein Teil der Beschwerden mit Auskunftsansprüchen Betroffener über die zu ihrer Person gespeicherten personenbezogenen Daten.

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

Nachdem der BGH in einem Urteil vom 15.06.2021 – Az. VI ZR 576/19 – bereits der Ansicht des EuGH gefolgt war, dass der Begriff personenbezogener Daten weit zu verstehen sei (Rn. 22), und eine sehr umfassende Pflicht zur Herausgabe von (Kopien von) personenbezogenen Daten bejaht hatte, veröffentlichte im Januar 2022 nun auch der Europäische Datenschutzausschuss (EDSA) einen ersten Entwurf für Leitlinien zum Recht auf Auskunft nach Artikel 15 DSGVO und gab diesen zur öffentlichen Konsultation frei. Auch der EDSA spricht sich darin für eine weite Auslegung des Auskunftsanspruchs für Betroffene aus.

Auffällig in unserer Aufsichtspraxis war, dass ein Teil der Betroffenen sich aber gerade darüber beschwerte, dass die an sie durch Verantwortliche meist elektronisch erteilten Auskünfte zu ihren personenbezogenen Daten dann derart umfangreich waren, dass die Betroffenen sich mit der Menge und der Kategorisierung der erteilten Information überfordert sahen.

3.2.2 Datenlöschung

Beinahe schon ein „Klassiker“ sind Beschwerden von Betroffenen, wonach zur Datenlöschung nach Artikel 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. Dies setzte sich auch im Berichtsjahr 2022 unvermindert fort.

In der Mehrzahl dieser Fälle konnte der Medienbeauftragte für den Datenschutz bei derartigen Beschwerden auch im Jahr 2022 feststellen, dass ein tatsächlicher Verstoß gegen datenschutzrechtliche Vorgaben der DS-GVO entgegen der Meinung der Beschwerden häufig 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, so dass 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 auch im Jahr 2022 häufig erst nach Einschaltung der Aufsicht vermitteln.

3.2.3 Cookie Banner und Consent Tools

Auch im Berichtszeitraum spielte das Thema der Ausgestaltung von *Cookie Bannern* bzw. *Consent Management Plattformen* (CMP) eine erhebliche Rolle. Dies hing einerseits mit der Arbeit der Task Force Banner wie auch der Bedeutung der nach wie vor häufig datenbasierten Online-Werbung wie auch Beschwerden dazu zusammen. Die Beschwerden zum Thema *Cookie Banner* bezogen sich auch im Jahr 2022 auf konkrete Angebote, bei denen nach Ansicht der Beschwerdeführer die Informationspflichten nicht ausreichend erfüllt, keine Ablehnmöglichkeit 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 hatten sich bei einem Großteil der Anbieter einheitliche Formulierungen auf Basis des „Transparency and Consent Framework 2.0“ (TCF 2.0) des Wirtschaftsverbandes der Onlinewerbebranche *iab* durchgesetzt. Unabhängig von der Tatsache, dass die Formulierungen durch das TCF vorgegeben werden, 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 graphische 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 graphische Gestaltung zur Abgabe einer Einwilligung zu verleiten oder gar zu bestimmen. Derartige Gestaltungen führen zu keiner wirksamen Einwilligung und machen erteilte Einwilligungen unwirksam. Da zahlreiche Verarbeitungsprozesse unter der Geltung des TTDSG nur mit einer wirksamen Einwilligung des Nutzers rechtmäßig sind, haben derartige Gestaltungen weitreichende Folgen.

In diesem Zusammenhang ist wie oben bereits erwähnt, auf die Beschwerdewelle des Vereins *noyb* mit europaweit 422 Beschwerden, von denen fünf in den Zuständigkeitsbereich des Medienbeauftragten für den Datenschutz fallen, und die deswegen eingesetzte Task Force Banner zu verweisen. Die fraglichen Beschwerden befassen

sich alle in unterschiedlicher Ausprägung mit der Frage der konkreten Gestaltung solcher Einwilligungsprozesse im Rahmen von *Cookie Bannern*. Auch die Frage des Widerrufs einer Einwilligung spielt dabei eine erhebliche Rolle.

Die Task Force kam im Jahre 2023 zu einer abschließenden Bewertung der vorgelegten Fragen, die auch die Billigung des EDSA fand. Gleichwohl wird das Thema wegen seiner grundlegenden Bedeutung gerade für die Gestaltung der Onlinewerbung unsere Aufsichtstätigkeit auch weiterhin stark prägen.

3.2.4 Werbung trotz Widerrufs

Wie auch in den vorangegangenen Berichtszeiträumen erreichten uns 2022 eine Reihe von Beschwerden, weil Betroffene von ihnen als unerfreulich empfundene Kontaktaufnahmen oder Zusendungen wie z. B. werbliche 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 Artikel 21 DS-GVO widersprochen hatten. In einigen Fällen war ihnen hierüber sogar eine entsprechende Bestätigung durch den Verantwortlichen zugegangen; dennoch erhielten die Petenten Anrufe, Briefe bzw. E-Mails oder wurden anderweitig Adressat werblicher Maßnahmen.

Auffällig und Ursache zahlreicher Beschwerden war folgende Fallgestaltung: Kunden eines Anbieters in unserem Zuständigkeitsbereich hatten im Berichtszeitraum immer wieder Probleme mit der Abmeldemöglichkeit bei Newslettern, da die in den Mails integrierten Abmeldelinks technisch nicht funktionierten und eine automatisierte Abmeldung von den Newslettern nicht zuließen. Aufgrund dieser Tatsache musste die Abmeldung manuell von Mitarbeitern des Verantwortlichen bearbeitet werden, wodurch es in zahlreichen Fällen zu zeitlichen Verzögerungen der Umsetzung der Widersprüche kam. Folge hiervon war, dass den Betroffenenrechten nicht fristgemäß nachgekommen wurde und an die Betroffenen für eine gewisse Zeit weitere Newsletter letztlich ohne Rechtsgrundlage versendet wurden. Der Mediendatenbeauftragte hat in diesen Fällen darauf hingewirkt, technisch-organisatorische Maßnahmen zu ergreifen, um das Problem abzustellen, was wohl auch erreicht werden konnte.

3.2.5 Datentransfer in Drittstaaten

Bis zur Entscheidung des EuGH vom 16. Juli 2020³³, die unter der Bezeichnung Schrems II bekannt wurde, konnte eine Datenübermittlung in die USA auf das EU-US-Datenschutzschild (Privacy Shield) bzw. den dieses betreffenden Durchführungsbeschluss der EU-Kommission³⁴ 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 bot aus Sicht des EuGH kein der EU im Wesentlichen gleichwertiges Schutzniveau. In der Folge wurde versucht, anderweitige Mechanismen zu entwickeln, die dieses Schutzniveau für den jeweiligen Einzelfall anderweitig herstellen wie z.B. über Standardvertragsklauseln i.S.d Art. 46 Abs. 2 lit. c DS-GVO³⁵.

Der Verein noyb – European Center for Digital Rights – legte bereits kurze Zeit nach dem Urteil im August 2020 101 Beschwerden gegen in der EU/EWR ansässige Unternehmen öffentlichkeitswirksam ein, da diese Anwendungen wie *Google Analytics* oder *Facebook Connect* auf Ihren Websites verwenden würden, so dass personenbezogene Daten an Google bzw. Facebook in den USA übermittelt würden, ohne dass dort ein angemessenes Schutzniveau für die übermittelten personenbezogenen Daten gewährleistet sei.

Auch uns hatte im September 2020 eine dieser 101 Beschwerden erreicht. Aufgrund der nahezu gleichgelagerten Sachverhalte und Beschwerden wurde im EDSA die Task Force „101 complaints“ gebildet, in der Vertreter aus zahlreichen EU-Mitgliedsstaaten kooperativ zusammenarbeiteten, um ein einheitliches Vorgehen abzustimmen und den Vorgaben der DS-GVO entsprechend ein möglichst einheitliches Datenschutzniveau in der EU herzustellen.

Die EDSA Task Force hatte Fragenkataloge ausgearbeitet, die die Grundlage auch unserer weiteren Tätigkeit in dieser Angelegenheit bildeten. Im Jahr 2022 erfolgten weitere Anhörungen aller Beteiligten, bei denen sich herausstellte, dass die Auffassungen doch nach wie vor erheblich voneinander abwichen. Das bei uns anhängige Verfahren berührt wegen der Einbindung des eingesetzten Facebook Tools und der damit einhergehenden Datentransfers, die letztlich wohl in den USA endeten, so viele

³³ EuGH Urteil vom 16.07.2020, C-311/18 - Schrems II <http://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=DE> (zuletzt abgerufen am 22.09.2023).

³⁴ 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.

³⁵ Vgl. Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates; Amtsblatt EU L 199/37.

grundlegende Fragen, dass das Verfahren im Berichtszeitraum noch nicht abgeschlossen werden konnte, was auch mit den unterschiedlichen beteiligten Datenschutzaufsichtsbehörden zusammenhing.

Die komplexen Fragestellungen rund um den Drittlandtransfer werden uns wie auch die anderen Aufsichtsbehörden in den kommenden Jahren weiter beschäftigen, auch wenn unterdessen das EU-US-Data Privacy Framework³⁶ ab 2023 eine neue Rechtsgrundlage schafft.

3.2.6 Tracking Tools

Auch im Berichtszeitraum erreichten den Mediendatenbeauftragten Beschwerden zum Einsatz von Tracking Tools auf unterschiedlichen Websites.

Mittels verschiedener Technologien ist es möglich, das Nutzungsverhalten auf Websites zu erfassen. Hierzu wurden in der Vergangenheit häufig Cookies eingesetzt, die es ermöglicht haben, den jeweiligen Nutzer wiederzuerkennen und so das Verhalten über längere Zeiträume zu erfassen und gegebenenfalls abzuspeichern. Beim Einsatz vom sogenannten *Cross-Site Tracking* oder *Third Party Cookies* war dies sogar über verschiedene Websites hinweg möglich. Moderne Webbrowser wie Safari verhindern werkseitig das *Cross-Site Tracking* sowie das Laden von *Third Party Cookies*. Auch andere Webbrowser wie etwa Edge oder Brave sind heutzutage so konfiguriert, so dass sie vom Werk aus bestimmte Tracker und Technologien blockieren, ohne dass es eines Zutuns des Nutzers (wie etwa dem Einsatz von Browser Add-ons) bedarf. Es ist absehbar, dass Tracking Tools künftig auf den Einsatz von Cookies verzichten (müssen), da diese mit hoher Wahrscheinlichkeit auf modernen Webbrowsern nicht mehr wie intendiert genutzt werden können. Bereits jetzt kommen sogenannte *Tracking Pixel* oder *Web Beacons* zum Einsatz, die auch ohne ein Cookie das Nutzungsverhalten aufzeichnen und an den Anbieter (der Website und/oder des Tracking Dienstes) weiterleiten können.

Wenn auf Websites Drittanbieter eingebunden werden, könnten diese das Nutzungsverhalten grundsätzlich auch über verschiedene Websites hinweg beobachten und dabei Nutzungsprofile erstellen. Nutzungsprofile werden unter anderem für das Auspielen von personalisierter Werbung genutzt. Aber auch weitere Einsatzmöglichkeiten sind vorstellbar.

³⁶ Commission Implementation Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

Bei der Einbindung von Drittanbietern, die die Nutzungsdaten auch für eigene Zwecke verwenden, ist eine Auftragsverarbeitung nicht mehr möglich. In diesen Fällen ist genau zu prüfen, ob der Nutzer ausreichend über diese Verarbeitung und die Rechtsgrundlage hierfür informiert wurde und ob eine rechtswirksame Einwilligung des Nutzers vorliegt.

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, aktuelle Fassung 1.1 vom Dezember 2022) hingewiesen, der sich der Medienbeauftragte für den Datenschutz inhaltlich angeschlossen hat.

3.3 Meldung von „Datenpannen“

3.3.1 Allgemeines zu Meldungen nach Artikel 33 DS-GVO

Sobald dem Verantwortlichen eine Verletzung des ihm aufgetragenen Schutzes personenbezogener Daten bekannt wird – umgangssprachlich wird auch von „Datenpannen“ gesprochen – besteht eine unverzügliche Meldepflicht gegenüber der zuständigen Aufsichtsbehörde gemäß Artikel 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.

Die Anzahl der uns im Berichtsjahr 2022 gemeldeten Datenschutzvorfälle war mit 34 gegenüber dem Vorjahr (75) stark rückläufig. Gleichwohl bildeten sie einen nicht unerheblichen Teil unserer täglichen Arbeit und nahmen viel Zeit in Anspruch, da stets der Einzelfall, die betroffenen Daten und die Umstände, die zur Verletzung des vorgesehenen Schutzes führten, untersucht werden müssen. In diesem Berichtszeitraum bildeten erneut Meldungen über Fehlversendungen und unbefugte Veränderungen von Bankdaten den Schwerpunkt.

3.3.2 Fehlversand

Mit weit mehr als der Hälfte den größten Anteil gemeldeter Datenschutzvorfälle gemäß Artikel 33 DS-GVO stellten auch im Berichtsjahr 2022 sogenannte Fehlversendungen, also die fehlerhafte Adressierung z. B. eines Briefes, Pakets oder einer E-Mail mit personenbezogenen Inhalten. Ihnen allen ist gemein, dass ein unberechtigter Dritter personenbezogene Daten einer anderen natürlichen Person erhielt. Festzustellen ist, dass der Anteil der Meldungen von Fehlversendungen sich weiterhin auf einem ähnlich hohen Niveau wie im Vorjahr bewegt.

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

3.3.3 Veränderung von Bankdaten

Mit einem Anteil von ca. 20% der uns gemeldeten Datenschutzvorfälle bildete auch in diesem Berichtsjahr die fehlerhafte bzw. falsch zugeordnete Eintragung von Bankdaten bei Kunden in Kundendatenbanken eine wichtige Kategorie

In solchen Fällen wurden häufig durch Kunden mitgeteilte Änderungen ihrer Bankdaten falsch zugeordnet und gleichzeitig bei anderen Kunden die dortigen Bankdaten fälschlich überschrieben. Folge ist eine unbefugten Veränderung von personenbezogenen Daten im Sinne von Art. 4 Nr. 12 DS-GVO.

Im Hinblick auf das Risiko finanzieller Schäden bei den Betroffenen und zur Vermeidung von Fehlbuchungen wurden Verantwortliche bei derartigen Sorgfaltspflichtverletzungen ermahnt, ihre Prozesse datenschutzkonform zu optimieren.

3.4 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 Artikel 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 Artikel 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.

Auch im Jahr 2022 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 Zusammenarbeit mit den Verantwortlichen für datenschutzkonforme Lösungen zu sorgen. Konkrete Abhilfebefugnisse des Art. 58

Abs. 2 DS-GVO standen daher nicht im Zentrum der Tätigkeit; hierbei ist zudem zu bedenken, dass die Mehrzahl der Verantwortlichen, die der Aufsicht des Mediendatenbeauftragten unterliegen, den Regelungen des Medienprivilegs nach Artikel 85 DS-GVO (vgl. hierzu näher 3.1.3) 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 durchgeführt und die hierzu eingegangenen Stellungnahmen ausgewertet.

In den meisten Fällen konnten auch im Berichtszeitraum 2022 bestehende Mängel bereits im Zuge der Anhörungen abgestellt und so eine datenschutzkonforme Verarbeitung schnell wiederhergestellt werden.

Bei 15 in 2022 abgeschlossenen Fällen (davon 10 gemeldete Datenpannen und 5 Beschwerden) 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 Berichtszeitraum nicht ausgesprochen.

Von der Möglichkeit der Verhängung von Geldbußen nach Artikel 83 DS-GVO hat der Mediendatenbeauftragte auch im Berichtszeitraum 2022 keinen Gebrauch gemacht.

3.5 Beratungstätigkeit und Fortbildungsveranstaltungen

Zu den Aufgaben des Medienbeauftragten für den Datenschutz gehört im Rahmen des allen Aufsichtsbehörden übertragenen Aufgabenkanons³⁷, die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten zu sensibilisieren ebenso wie die breite Öffentlichkeit, insbesondere Kinder und Jugendliche, rund um das Thema Datenschutz zu informieren im Rahmen entsprechender Veranstaltungen wie auch mit geeigneten Materialien.

Dieser Aufgabe des Sensibilisierens nimmt sich der Mediendatenbeauftragte einerseits im Rahmen der unter 3.1 beschriebenen Anfragen einzelner Verantwortlicher

³⁷ Das Europarecht weist den Aufsichtsbehörden nach Art. 51 DS-GVO zahlreiche Aufgaben von der Information der Öffentlichkeit und der Sensibilisierung für Risiken und Rechte, über die Überwachung der Einhaltung der gesetzlichen Vorgaben und ihre Durchsetzung, bis zur Entwicklung von Standardvertragsklauseln, Verhaltensregeln und Datenschutz Zertifizierungsmechanismen zu, vgl. insbesondere Art. 57 Abs. 1 DSGVO.

und andererseits durch an die Allgemeinheit gerichtete Veranstaltungen und Veröffentlichungen an.

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*, zu den Möglichkeiten einer Cookie-freien Gestaltung oder zum Thema *Consent Tools*.

Daneben fand ein regelmäßiger Austausch auch mit der Datenschutzbeauftragten der BLM zu unterschiedlichen Themen, insbesondere zur Gestaltung von *Cookie Bannern* und *Consent Tools*, statt.

Der Medienbeauftragte für den Datenschutz und sein Team nahmen an verschiedenen juristischen Fortbildungsveranstaltungen, Fachveranstaltungen aus dem Datenschutzbereich und der Datenschutzcommunity, wie beispielsweise den Bayerischen Datenschutztagen und den Gunzenhausener IuK-Tagen, sowie fachübergreifenden Tagungen teil. Ebenso fanden im Jahr 2022 erstmals wieder die von der Medien.Bayern GmbH veranstalteten Lokalfunkstage in Nürnberg, der jährliche Branchentreff, ebenso wie eine der maßgeblichen Veranstaltungen für die Medienbranche, die Medientage München, unter der Beteiligung des Mediendatenbeauftragten und seines Teams statt.

Die im Jahr 2020 ins Leben gerufene Workshopreihe zur Ausgestaltung von Onlineangeboten und aktuellen gesetzlichen Entwicklungen konnte im Berichtsjahr mit einer in Präsenz und gleichzeitig online stattfindenden Veranstaltung zum neuen TTDSG fortgesetzt werden.

Aufgrund der im Jahre 2022 reduzierten Besetzung des Teams des Mediendatenbeauftragten konnten eigene – insbesondere an die breite Öffentlichkeit gerichtete Veranstaltungen – nur in sehr geringem Rahmen umgesetzt werden.

3.6 Zahlen und Fakten im Überblick

Auch im Jahr 2022 blieb zwar die Anzahl der Beratungen, Beschwerden und gemeldeten Datenschutzverletzungen auf konstant hohem Niveau wie auch im Vorjahr. Gleichzeitig setzte sich ein Trend aus dem Jahr 2021 fort: Es 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 auch in 2022 einige zu thematischen Schwerpunktfällen, die das Team des Medienbeauftragten für den Datenschutz mit einer

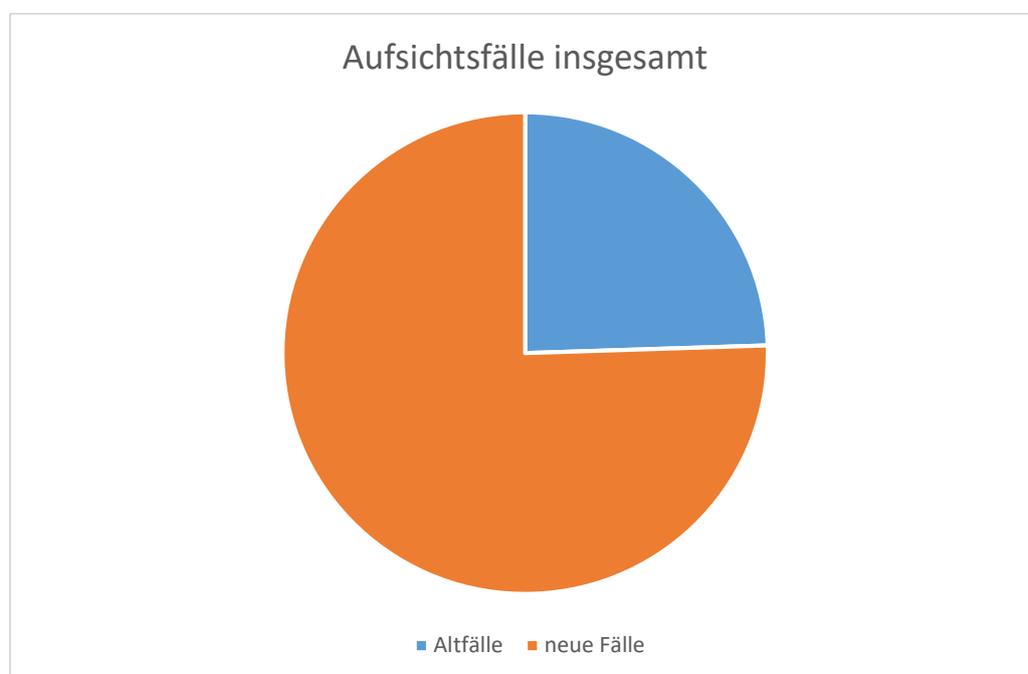
intensiven iterierenden Bearbeitung über einen längeren Zeitraum in Anspruch nahmen.

Dazu kam, dass sich das Verhältnis der Aufsichtsfälle untereinander stark veränderte: So hat sich die Anzahl der Anfragen und der Kontrollanregungen mehr als verdoppelt. Dahingegen ist die Anzahl der gemeldeten Datenschutzverletzungen auf ungefähr die Hälfte im Vergleich zum Jahr 2021 zurückgegangen. Die Anzahl der Beschwerden blieb gleich und weiterhin hoch. Ebenso wurden mehr Fälle aus dem Vorjahr mit ins Jahr 2022 mitgenommen, da diese in 2021 nicht abgeschlossen werden konnten.

Schwerpunktt Themen waren bei den Beschwerdefällen vor allem die Datenlöschung und der Versand von Werbung trotz eines Widerspruchs bzw. einer vorgeblichen Datenlöschung/-sperrung. Bei den gemeldeten Datenschutzverletzungen nahmen unter anderem Fehlversandfälle weiterhin einen großen Raum ein, bei denen personenbezogene Daten von betroffenen Personen gegenüber unbefugten Dritten offengelegt wurden.

Am Ende des vorangegangenen Berichtszeitraumes 2021 waren noch insgesamt 48 Verfahren aus den Vorjahren offen und wurden im aktuellen Berichtszeitraum 2022 weiter bearbeitet.

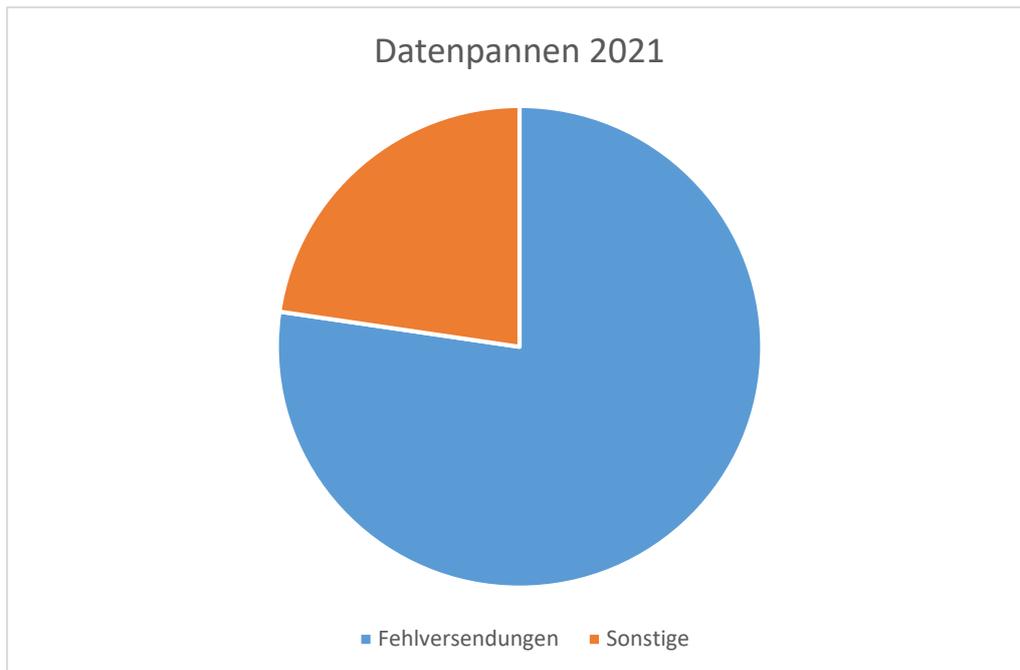
Zu den genannten Verfahren kamen im Jahr 2022 insgesamt 148 neu eingeleitete Verfahren hinzu.





Die gemeldeten Datenschutzverletzungen belaufen sich in 2022 auf 34, die Anzahl der Beschwerden beläuft sich auf 56. Zudem wurden 18 Kontrollanregungen zugeleitet. Die Anzahl der Anfragen stieg sehr deutlich auf 40.

Vorrangig handelte es sich bei den uns gemeldeten Datenschutzverletzungen leider nach wie vor zum großen Teil um Fehlversendungen, deren Inhalt von belangloseren Werbemails bis hin zu gesamten Vertragsunterlagen, Bankdaten und vollständigen Datenauskünften alles umfasste. Häufig war menschliches Versagen die Ursache der Verletzung. Zumeist lassen sich auch keine anderen Gründe ermitteln.



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.

Dauerthemen im Jahr 2022 waren wie auch in den Vorjahren Datenverarbeitungen trotz Widerrufs insbesondere für Werbezwecke und vorgeblich bzw. tatsächlich nicht umgesetzte Löschersuchen; in der Regel waren allerdings die gesetzlich vorgeschriebenen Aufbewahrungsfristen noch nicht abgelaufen, so dass einstweilen nur eine Sperrung erfolgen konnte. Die Beschwerden bzgl. Tracking und Cookies hingegen waren eher rückläufig.

Die Anzahl der Anfragen stieg deutlich im Vergleich zum Vorjahr von 19 auf 40 im Jahr 2022. Inhaltlich betrafen sie neben aktuellen Entwicklungen unterschiedlichste Fragen aus verschiedensten Bereichen des Datenschutzrechtes bis hin zu den Besonderheiten des Medienprivilegs.

Hinzu kommen allerdings noch zahlreiche weitere Anfragen, die kurzfristig in Ad-Hoc-Beratungen geklärt werden konnten und nicht eigens gezählt wurden.

3.7 Ausblick

Seit der Geltung der DS-GVO im Mai 2018 kann der Mediendatenbeauftragte auf eine von Jahr zu Jahr steigende Anzahl an eingehenden Beratungsanfragen, Beschwerden zu Datenschutzverletzungen sowie gemeldeten Datenpannen zurückblicken. Im Jahr 2022 konsolidierte sich die Anzahl in etwa auf dem Niveau des Vorjahres.

Abschluss der Task Forces

Neben den Beschwerden, Anfragen und Datenpannen rückte im Berichtsjahr gleichzeitig die Mitarbeit auf europäischer Ebene in den Task Forces „Banner“ und „101 Beschwerden“ deutlich in den Vordergrund und wurde auch durch die Einführung des neuen TTDSG nochmal anders bedeutsam und gewichtig. Dies führte zur zeitlich intensiven Einbindung und Mitarbeit in den Task Forces einerseits und zur stärkeren Zusammenarbeit mit den nationalen und europäischen Datenschutzaufsichten und Datenschutzinstitutionen andererseits. Diese Arbeit in den Task Forces und der verstärkte Austausch mit den anderen Behörden kam in 2022 zu ihrem Höhepunkt; die wesentliche Arbeit dieser Task Forces fand im Jahr 2022 statt. Direkt zu Beginn des Jahres 2023 konnte die Task Force Banner mit der Veröffentlichung eines Berichts³⁸ abgeschlossen werden. Auch die Task Force 101 Beschwerden sollte im Jahr 2023 einen entsprechenden Abschluss finden.

Austausch mit der Verbraucherzentrale Bayern

Aus der Arbeit in den Task Forces und den dort schwerpunktmäßig behandelten Themen, allen voran das Thema *Cookie Banner*, wurde zum Ende des Jahres 2022 die Wiederaufnahme des Austauschs mit der Verbraucherzentrale Bayern zu aktuellen Themen in die Wege geleitet.

Fortsetzung der Workshopreihe

Aufgrund der reduzierten Besetzung des Teams des Medienbeauftragten für den Datenschutz konnte im Jahr 2022 leider nur ein Anbieterworkshop durchgeführt werden. Zudem zeigte sich eine gewisse Vorsichtigkeit bei Präsenzveranstaltungen, persönlichem Kontakt und Austausch bedingt durch die Auswirkungen der Corona-Pandemie. So schien die Durchführung entsprechender Veranstaltungsformate noch als

³⁸ https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf (zuletzt abgerufen am 08.08.2023).

schwierig. Nach wie vor nahmen an dieser Stelle Online-Meetings, telefonischer Austausch und eine entsprechende Beratung einen großen Raum ein.

Aus den in 2022 in den Task Forces behandelten Themen und den damit zusammenhängenden Entschlüssen der DSK zum Ende des Berichtsjahres wird sich im Jahr 2023 die thematische Schwerpunktsetzung für die Fortsetzung der Workshopreihe für Anbieter ergeben. Im Mai 2023 konnte der nächste Termin in der BLM stattfinden. Ein weiterer ist derzeit für den Herbst 2023 geplant.

Schwerpunktuntersuchung Websites

Der Mediendatendatenbeauftragte plant für das Jahr 2023 eine Schwerpunktuntersuchung vorzubereiten. Seit der letzten Untersuchung gab es mehrere grundlegende Veränderungen: Das TTDSG ist in Kraft getreten und hat klare Regeln für den Zugriff auf und das Speichern von Informationen auf Endgeräten von Nutzern aufgestellt; infolgedessen hat die Datenschutzkonferenz ihre Orientierungshilfe für Anbieter von Telemedien angepasst und aktualisiert; zudem hat die Taskforce Banner des Europäischen Datenschutzausschusses Anfang 2023 ihren Abschlussbericht veröffentlicht und problematische Gestaltungen von Cookie Bannern aufgezeigt.

Anbieter von Websites hatten nunmehr die Gelegenheit die Gestaltung ihrer Websites sowohl in technischer als auch in graphischer Hinsicht zu untersuchen und ggf. diese dergestalt anzupassen, dass diese auch den geltenden gesetzlichen Regeln entsprechen. Inwiefern die Anbieter ihre Websites inzwischen umgestellt haben, soll mithilfe der geplanten Schwerpunktuntersuchung ermittelt werden.

Darüber hinaus wird auch die Untersuchung von HbbTV-Angeboten in Erwägung gezogen, da auch dort die rechtlichen Vorgaben aus dem TTDSG und der DS-GVO gelten, und zu ähnlichen, gelegentlich auch spezielleren Anforderungen und Antworten führen.

EU-US-Data Privacy Framework

Eine zentrale datenschutzrechtliche Herausforderung ergab sich im Hinblick auf die Frage, ob und wenn ja, unter welchen Bedingungen, unter die Geltung der DS-GVO fallende personenbezogene Daten rechtmäßig in die USA transferiert werden könnten, seit der EuGH³⁹ im Jahr 2015 den seinerzeitigen Angemessenheitsbeschlusses

³⁹ Urteil des EuGH vom 6. Oktober 2015 (Rechtssache C 362/14 - „Schrems 1“).

der EU Kommission⁴⁰ aufhob, der zuvor die hierfür erforderliche Rechtsgrundlage darstellte. Dieses Frage blieb auch danach virulent, da das als neue Rechtsgrundlage geschaffene EU-US Privacy Shield von Anfang an berechtigten Zweifeln begegnete und dann im Jahr 2020 ebenfalls vor dem EuGH⁴¹ scheiterte. Nach intensiven Verhandlungen traf der amerikanische Präsidenten in 2022 eine Anweisung an seine Geheimdienste zu deren künftigem Vorgehen; im Jahr 2023 wurde sodann das EU-US-Data Privacy Framework⁴² abgeschlossen, das nunmehr für Europäer in den USA ein vergleichbares Datenschutzniveau herstellen soll.

Auch wenn gewisse Fortschritte für die Rechte von Europäern nicht zu leugnen sind, wird nach wie vor bezweifelt, dass damit wirklich ein vergleichbares Datenschutzniveau bereits erreicht ist. Der EDSA hat hierzu eine wohl im Wesentlichen positive Stellungnahme abgegeben. Die europäische Kommission hat daraufhin ein weiteres Mal ein angemessenes Schutzniveau attestiert. Gleichwohl wurden umgehend entsprechende Klageverfahren angekündigt. Ob das Privacy Framework eine tragfähige Rechtsgrundlage für die dauerhaft und ständig stattfindenden Datentransfers in die USA bilden wird, bleibt abzuwarten.

In diesen und allen anderen inhaltlichen Datenschutzfragen wird sich der Medienbeauftragte und sein Team weiterhin nach Kräften bemühen, 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 beitragen, künftige datenschutzrechtliche Probleme rechtzeitig zu erkennen und möglichst frühzeitig zu entschärfen oder auch zu lösen.

⁴⁰ Entscheidung der EU-Kommission vom 6.7.2000, dass die seinerzeit geltenden „Safe-Harbour Bedingungen“ in den USA unter bestimmten Voraussetzungen ein den europäischen Standards vergleichbares Schutzniveau schaffen würden.

⁴¹ „Schrems II“-Urteil des EuGH vom 16.7.2020 in der Rechtssache C 311/18.

⁴² Vgl. COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

Sensibilisierung der Öffentlichkeit

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 und Informationsmaterialien angeboten werden.

Prüfungen und Kontrollmaßnahmen

Zudem werden in der folgenden Berichtsperiode Prüfungen und Kontrollmaßnahmen wieder an Bedeutung gewinnen. Diesen vorgelagert sind anbieterübergreifende Basisuntersuchungen, die bereits in einem gewissen Umfang stattfinden und die Aufgabe haben, einen Überblick über die Marktgegebenheiten im Zuständigkeitsbereich zu vermitteln. Aus diesen Untersuchungen ergeben sich wiederum in erster Linie Aufschlüsse über konkrete Bedarfe für Unterrichtungen und Informationsveranstaltungen, aber auch gegebenenfalls für die Einleitung von Aufsichtsverfahren.

Gleichwohl wird die Grundausrichtung der Aufsichtstätigkeit unverändert vor allem darin liegen, die gesetzlichen Vorgaben bekanntzumachen, sie zu erklären, danach aber auch auf deren Einhaltung zu drängen.