BLM
Bayerische
Landeszentrale für
neue Medien

# 1. Tätigkeitsbericht

# des

# Medienbeauftragten für den Datenschutz

## bei der Bayerischen Landeszentrale für neue Medien

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

# Vorbemerkung

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

Mit Geltung der Datenschutzgrundverordnung (DS-GVO) am 25. Mai 2018 eröffneten sich auch für die in den Zuständigkeitsbereich des Medienbeauftragten für den Datenschutz fallenden Einrichtungen zahlreiche Neuerungen und Veränderungen. Für den Mediendatenbeauftragten selbst ergaben sich dadurch strukturelle Änderungen: Das Team konnte im Berichtszeitraum um zwei Referentenstellen in 2018 und eine halbe Assistentenstelle in 2019 erweitert werden, und so eine funktionstüchtige Aufsichtsinstitution aufgebaut werden. Ende 2019 wurden Vorbereitungen für die Besetzung einer weiteren halben Referentenstelle zum Jahresbeginn 2020 getroffen.

Aufgrund dieser so verbesserten Aufstellung des Medienbeauftragten für den Datenschutz gibt dieser Bericht zunächst einen Überblick über seine Positionierung, Aufgaben und Tätigkeitsbereiche, bevor ein Blick auf aktuelle gesetzliche Entwicklungen in Datenschutzfragen für den Medienbereich geworfen wird: Hier sind vor allem die Urteile des Europäischen Gerichtshofs (EuGH) zu den *Facebook Fanpages* sowie zu *Fashion ID* und *Planet 49* als relevant für die Aufsichtstätigkeit zu erwähnen. Aber auch die Veröffentlichung der *Orientierungshilfe der staatlichen Aufsichtsbehörden für die Anbieter von Telemedien* war im Berichtszeitraum für uns zentral, da deren Inhalte die Grundlage für die für das Jahr 2020 geplante Workshopreihe für die Anbieter bilden.

Im Anschluss erläutern wir unsere Aktivitäten anhand von Fallbeispielen: Neben Anfragen zum Thema *One Stop Shop*, zur Erstellung von Datenschutzerklärungen und zum Medienprivileg beschäftigten uns zahlreiche Beschwerden und Kontrollanregungen, wie beispielsweise zu den Themen Auskunftsanspruch, Datenlöschung, Verschlüsselung und *Tracking Tools*. Schließlich nahmen die sogenannten Datenpannen häufig aufgrund von Fehlversendungen wie auch in Verbindung mit den Themen *Phishing* und Trojaner, verlorene Datenträger und offene E-Mailverteiler einen großen Teil unserer Aufsichtstätigkeiten ein. Einige relevante Zahlen und Fakten zu unseren Tätigkeiten liefern einen abschließenden Überblick und leiten zum Ausblick ins neue Jahr 2020 über.

Der vorliegende Bericht soll allen Interessierten einen Einblick in unsere Aufgaben und Tätigkeitsfelder liefern und gleichsam auch die Schwerpunkte unserer Arbeit in dieser Berichtsperiode herausstellen. Er ist der erste des Medienbeauftragten für den Datenschutz, der nach Geltung der Datenschutz-Grundverordnung erstellt wird. Daher bezieht er sich auf den Zeitraum ab dem 25.05.2018, seit dem die Datenschutz Grundverordnung verbindlich zu beachten ist, bis zum regulären Ende des Jahres 2019.

München, 09.06.2020

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

# Inhalt

# 1. Der Medienbeauftragte für den Datenschutz und seine Aufgaben

## 1.1 Rechtliche Einordnung als Aufsicht

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

*Mediendatenbeauftragter (MDB)* wird im Folgenden verwendet als Abkürzung für die Bezeichnung *Der Medienbeauftragte für den Datenschutz* .

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

Die Bayerische Landeszentrale für neue Medien wird im Text mit Landeszentrale oder BLM abgekürzt.

Der Mediendatenbeauftragte überwacht bei diesen Stellen die Einhaltung der Vorgaben des Datenschutzrechts. Sein sektorspezifischer Zuständigkeits- und Aufsichtsbereich ist dort aber nicht auf die Überwachung der Einhaltung der speziell für den Medienbereich geltenden – oder besser: die meisten Regelungen der DS-GVO ersetzenden – Datenschutzvorschriften beschränkt (vgl. hierzu insbesondere die Vorgaben zum sogenannten *Medienprivileg* (s. 3.1.3) des Art. 85 DS-GVO). Im Gegenteil: Er ist bei den oben genannten Stellen sowie ggf. im Rahmen des sogenannten *One-Stop-Shop* auch bei Tochterunternehmen von Anbietern (vgl. 3.1.1) umfassend für die Überwachung jeglicher datenschutzrechtlich relevanter Vorgänge zuständig.

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

1 Überall dort, wo es möglich war, wurden geschlechtsneutrale Formulierungen verwendet. Ansonsten wurde auf das generische Maskulinum zurückgegriffen. Dort, wo es bedeutungstragend war, wurden die jeweiligen geschlechtsspezifischen Formen angewandt.

## 1.2 Aufgaben und Befugnisse

Die Aufgaben und Befugnisse des Mediendatenbeauftragten ergeben sich insbesondere aus Art. 57, 58 Abs. 1-5 DS-GVO. Er verfügt also 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 Anweisungsbefugnisse) bis hin zur Sanktion der Verhängung von Geldbußen nach Art. 83 DS-GVO als „schärfstem Schwert" der nach der DS-GVO vorgesehenen Maßnahmen reichen. Eine Einschränkung besteht lediglich im Hinblick auf die BLM, der gegenüber keine Geldbußen vorgesehen sind (Art. 20 Abs. 6 Satz 3 BayMG).

## 1.3 Zusammenarbeit mit anderen Behörden und Institutionen

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

www.lda.bayern.de

www.datenschutz-bayern.de

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

https://www.katholisches-datenschutzzentrum.de/wir-ueber-uns/konferenz-der-dioezesandatenschutzbeauftragten/

https://datenschutz.ekd.de/

https://www.diakonie.de/datenschutz/

https://datenschutz.ekd.de/vernetzung/andere-evangelisch/

Für die bayerischen Datenschutzaufsichtsbehörden sieht Art. 21 BayDSG vor, dass sie regelmäßig die in Erfüllung ihrer Aufgaben gewonnen Erfahrungen austauschen und sich gegenseitig in ihrer Aufgabenwahrnehmung unterstützen. In Erfüllung dieser Vorgabe fanden insbesondere mit dem *Bayerischen Landesamt für Datenschutzaufsicht* im Berichtszeitraum ein reger Austausch zu unterschiedlichsten Aufsichtsfragen sowie wechselseitig zuständigkeitsbedingte Abgaben statt.

# 2. Interessante Entwicklungen im Fokus

## 2.1 Wichtige gesetzliche Änderungen und Vorhaben

Nachdem auf Bundesebene bereits im Jahr 2017 das Bundesdatenschutzgesetz (BDSG) durch eine Novellierung auf die Vorgaben der DS-GVO angepasst worden war, trat am 26.11.2019 das „Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU)" in Kraft. Neben einer Vielzahl von Änderungen in einzelnen bereichsspezifischen Datenschutzregelungen zur Anpassung an die DS-GVO entfaltete vor allem eine wichtige Änderung im BDSG relevante Auswirkungen auch für die der Aufsicht des Medienbeauftragten für den Datenschutz unterliegenden Anbieter und Beteiligungsunternehmen der BLM: Seitdem besteht die Pflicht zur Benennung eines Datenschutzbeauftragten bei nichtöffentlichen Stellen grundsätzlich erst ab 20 Beschäftigten (vormals zehn), d. h. wenn 20 oder mehr Mitarbeiterinnen und Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Diese organisatorische Erleichterung darf jedoch nicht zu der Annahme führen, dass dann in kleineren Unternehmen kein Datenschutzrecht mehr gelte. Die gesetzlichen Vorgaben des Datenschutzes sind selbstverständlich auch von den Unternehmen weiterhin zu beachten, die diesen Schwellenwert unterschreiten. Zudem besteht unabhängig von der Anzahl der mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen weiterhin eine Benennungspflicht für eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten in den in Art. 35 und Art. 37 der DS-GVO sowie den in § 38 BDSG ausdrücklich genannten Fällen (z. B. Verarbeitungen, die einer Datenschutz-Folgenabschätzung unterliegen oder Datenverarbeitung für Zwecke der Markt- oder Meinungsforschung).

Ein betrieblicher Datenschutzbeauftragter ist seit 26.11.2019 in der Regel erst ab 20 Mitarbeitern erforderlich. Die Regeln der DS-GVO gelten aber für alle Betriebe – unabhängig von ihrer Betriebsgröße.

Zumindest vorläufig zum Erliegen kamen hingegen auf EU-Ebene Ende 2019 die Verhandlungen für die umstrittene ePrivacy-Verordnung für den Datenschutz in der elektronischen Kommunikation. Nach dem Willen der EU-Kommission sollte diese ursprünglich bereits im Mai 2018 die Datenschutzrichtlinie für elektronische Kommunikation aus dem Jahr 2002 (ePrivacy-Richtlinie 2002/58/EG) ablösen und parallel mit der DS-GVO in Kraft treten. Sie sollte in Ergänzung und Überlagerung der Vorschriften der DS-GVO insbesondere Kommunikationsvorgänge und den Datenschutz im

Bereich der elektronischen Kommunikation und damit auch im Bereich sozialer Netzwerke regeln. Nach erheblichem Widerstand vor allem seitens der Online-Werbewirtschaft, die ihre Geschäftsmodelle durch eine Verschärfung der Anforderungen an die Erstellung von Nutzerprofilen und Webtracking in Gefahr sieht, kamen die Konsultationen auf politischer Ebene zum Stillstand. Ein neuer Gesetzentwurf der EU-Kommission wurde Ende 2019 für das Jahr 2020 zwar angekündigt, aber aufgrund der erforderlichen Trilog-Verhandlungen und einer sich daran anschließenden Umsetzungsfrist von zwei Jahren ist zum Redaktionsschluss dieses Berichts mit einem Inkrafttreten frühestens für das Jahr 2023 zu rechnen. Dies ist eine sehr unglückliche Situation: Fragen des Nutzer-Tracking für zielgerichtete Werbung, des Setzens von Cookies bzw. der Umgang mit bestimmten Meta-Daten bleiben so vorerst ungeregelt bzw. unabgestimmt mit den insoweit lückenhaften Regelungen der neuen DS-GVO und unterfallen weiterhin dem von vielen als „veraltet" empfundenen Regelungsrahmen der ePrivacy-Richtlinie.

## 2.2 Gemeinsam Verantwortliche

Bereits mit Urteil vom 5.6.2018 und noch zur Rechtslage der durch die DS-GVO abgelösten Datenschutz-Richtlinie (Richtlinie 95/46/EG) hatte der EuGH (Rechtssache C-210/16, „Wirtschaftsakademie Schleswig-Holstein") entschieden, dass der Betreiber einer Facebook Fanpage gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Besucher seiner Seite verantwortlich ist.

Fanpages sind Benutzerkonten, die bei Facebook von Privatpersonen oder Unternehmen eingerichtet werden können. Der Fanpage-Anbieter kann nach einer Registrierung bei Facebook seine Plattform dazu nutzen, sich den Nutzern dieses sozialen Netzwerks sowie Personen, die die Fanpage besuchen, zu präsentieren und Äußerungen aller Art in den Medien- und Meinungsmarkt einzubringen. Die Betreiber von Fanpages können mit Hilfe der Funktion *Facebook Insight*, die ihnen Facebook als nicht abdingbaren Teil des Benutzungsverhältnisses kostenfrei zur Verfügung stellt, anonymisierte statistische Daten betreffend die Nutzer dieser Seiten erhalten. Diese Daten werden mit Hilfe von Cookies gesammelt, die jeweils einen eindeutigen Benutzercode enthalten, der für zwei Jahre aktiv ist und den Facebook auf der Festplatte des Computers oder einem anderen Datenträger der Besucher der Fanpage speichert – und zwar unabhängig davon, ob diese Person

über ein Facebook-Konto verfügt oder nicht. Der Benutzercode, der mit den Anmeldedaten solcher Nutzer, die bei Facebook registriert sind, verknüpft werden kann, wird beim Aufrufen der Fanpages erhoben und verarbeitet.

Durch die Einrichtung einer Fanpage auf Facebook von Seiten ihres Betreibers trägt dieser zur Verarbeitung der personenbezogenen Daten der Besucher seiner Seite bei. Er ist daher an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt und so gemeinsam mit Facebook als für diese Verarbeitung Verantwortlicher einzustufen. Die datenschutzrechtliche Verantwortlichkeit für Facebook Fanpages liegt also nicht allein bei Facebook.

Allerdings können nach dem EuGH beide Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.

Mit seinem die Maßgaben des EuGH umsetzenden Urteil hat das Bundesverwaltungsgericht (BVerwG) am 11.09.2019 entschieden (Az. 6 C 15.18), dass eine Aufsichtsbehörde in solchen Fällen im Wege der Ermessensausübung nicht unbedingt gegen Facebook vorgehen muss, sondern aus Gründen der Gefahrenabwehr auch lediglich den Betreiber der Fanpage als gemeinsam Verantwortlichen in die Pflicht nehmen kann. Da die Feststellungen des vormals mit der Angelegenheit befassten Berufungsgerichts (OVG Schleswig) aber nach Ansicht des BVerwG nicht ausreichten, um die Rechtmäßigkeit der Datenverarbeitungsvorgänge selbst zu beurteilen, hat es noch keine Entscheidung über die Zulässigkeit der eigentlichen Datenverarbeitung getroffen und die Sache zur anderweitigen Verhandlung und Entscheidung an das Berufungsgericht zurückverwiesen.

Diese Urteile sind zwar noch zur „alten" Rechtslage ergangen. Die Rechtsprechung ist gleichwohl auf die DS-GVO übertragbar, da der – weit auszulegende – Begriff des Verantwortlichen in der DS-GVO insoweit keine Änderung erfahren hat.

Mit den oben genannten Urteilen ist trotz der noch für den konkreten Einzelfall zu berücksichtigenden Details nunmehr klagestellt, dass jeder Fanpage-Betreiber selbst sicherstellen muss, dass – im Rahmen seiner (Mit-) Verantwortung – die Datenverarbeitung rechtmäßig im Sinne des Art. 6 DS-

GVO erfolgt und er als (Mit-)Verantwortlicher auch seiner Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nachkommen muss. Im Ergebnis kann er dieser Verpflichtung bei den Facebook Fanpages in der Regel nur mittels hinreichender „Joint-Controller"-Vereinbarung mit Facebook nach Art. 26 DS-GVO nachkommen.

Im Zuge des EuGH-Urteils stellte Facebook hierzu zwar eine „Seiten-Insights-Ergänzung" für den Geltungsbereich der DS-GVO zur Verfügung, behält sich jedoch weiterhin die alleinige Entscheidungsmacht vor, wie es seine Pflichten gemäß dieser Seiten-Insights-Ergänzung erfüllt. Ob ein Fanpage-Betreiber unter diesen Voraussetzungen seinen eigenen datenschutzrechtlichen Transparenz-, Rechtmäßigkeits- und Nachweisverpflichtungen aus der DS-GVO nachkommen kann, ist nach derzeitigem Stand mehr als fraglich.

## 2.3 Urteile zu Fashion ID und Planet 49 : Herausforderungen für die Aufsichtspraxis

### 2.3.1 Fashion ID

Eine weitere wichtige Entscheidung zur gemeinsamen Verantwortlichkeit – und ebenfalls noch zur Rechtslage der durch die DS-GVO abgelösten Datenschutzrichtlinie – traf der EuGH im Berichtszeitraum zur Einbindung sogenannter *Social Media Plugins* auf Websites (EuGH, Urteil vom 29.07.2019, Rechtssache C-40/17, „Fashion-ID") ebenfalls auf ein Vorabentscheidungsersuchen eines deutschen Gerichtes hin, in diesem Fall des OLG Düsseldorf. Im konkreten Fall ging es um die Einbindung des Facebook Like-Buttons. Durch die Einbindung dieses Plugins werden Daten der Websitebesucher an Facebook als Dritten übertragen, wobei Facebook anschließend die übertragenen Daten auch zu eigenen Zwecken nutzen kann.

Über die Zwecke und Mittel entscheidet bei der gemeinsamen Verantwortlichkeit grundsätzlich nicht nur eine Partei, wobei die Beteiligung der Parteien an den gemeinsamen Entscheidungen jedoch verschiedene Formen aufweisen kann und nicht gleichmäßig verteilt sein muss (vgl. dazu oben sowie schon WP 169 der ARTIKEL-29-DATENSCHUTZGRUPPE, S. 23).

Der EuGH äußerte sich in seinem Urteil vom 29.07.2019 erneut näher zur Reichweite der gemeinsamen Verantwortung: Demnach kann der Betreiber einer Website, der in diese Website ein Social Plugin einbindet, das den

Browser des Besuchers dieser Website veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten des Besuchers an diesen Anbieter zu übermitteln, als für die Verarbeitung Verantwortlicher im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 angesehen werden. Diese Verantwortlichkeit ist jedoch auf den Vorgang oder die Vorgänge der Datenverarbeitung beschränkt, für den bzw. für die er tatsächlich über die Zwecke und Mittel entscheidet, d. h. hier das Erheben der in Rede stehenden Daten und deren Weitergabe durch Übermittlung, die durch Aufruf der eigenen Seite initiiert werden. Nicht verantwortlich ist der Betreiber der Website jedoch für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die er weder die Zwecke noch die Mittel festlegt. Den Betreiber einer solchen Website trifft in einer solchen Situation auch die in dieser Bestimmung vorgesehene Informationspflicht, wobei dieser die betroffene Person auch hier nur in Bezug auf den Vorgang oder die Vorgänge der Verarbeitung personenbezogener Daten informieren muss, für den bzw. für die dieser Betreiber tatsächlich über die Zwecke und Mittel entscheidet. Gleiches gilt dann für die von einer betroffenen Person durch den Betreiber gegebenenfalls einzuholende Einwilligung, soweit sich der Betreiber sowie der Plugin-Anbieter nicht jeweils bereits auf ein berechtigtes Interesse berufen kann. Soll sich die Rechtfertigung für die Verarbeitung personenbezogener Daten aus einem solchen Interesse ergeben, muss diese Verarbeitung zur Verwirklichung des berechtigten Interesses auch tatsächlich erforderlich sein. Zudem dürfen keine Interessen, Grundrechte und Grundfreiheiten der betroffenen Person erkennbar sein, die die berechtigten Interessen des Verantwortlichen überwiegen.

Zwingend erforderlich ist eine auf der Grundlage von klaren und umfassenden Informationen erteilte Einwilligung des Nutzers jedoch, soweit der Anbieter eines Social Plugins über dieses Zugriff auf Informationen hat, die im Endgerät des Besuchers der Website des Betreibers gespeichert sind. Dies sieht die aufgrund des bisherigen Scheiterns der ePrivacy-Verordnung (siehe 2.1) weiterhin geltende Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie 2002/58/EG) vor.

### 2.3.2 Planet 49

Der EuGH hat mit seiner im Oktober 2019 verkündeten Entscheidung in der Rechtssache Planet 49[2] ein drittes Mal auf eine Anfrage eines deutschen Gerichtes hin im Berichtszeitraum ein zukunftsweisendes Urteil gefällt. Diesmal stand vor allem die Frage im Zentrum, welche Voraussetzungen für eine Einwilligung vorliegen müssen bzw. wann eine Einwilligungserklärung angenommen werden kann.

Zum Hintergrund:

In dem vom Bundesgerichtshof (BGH) zu entscheidenden Fall ging es im Rahmen eines Gewinnspiels um eine Einwilligungserklärung, die u. a. das Setzen von Cookies zum Zwecke der Werbung des Website-Betreibers sowie dessen Kooperationspartnern zum Gegenstand hatte. Die konkrete Einwilligungserklärung war mit einem Kästchen versehen, in dem das Häkchen bereits gesetzt war. Der Internetnutzer musste selbst aktiv werden und das Häkchen entfernen, um der Analyse seines Verhaltens durch den vom Website-Betreiber eingeschalteten Analysedienst zu entgehen.

Nachlese: Der BGH hat am 28.05.2020 dazu sein Urteil (**I ZR 7/16**) verkündet. Weitere Informationen finden sich in der Pressemitteilung: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html?nn=10690868 (abgerufen am 09.06.2020)

In erster Instanz (LG Frankfurt/M., MMR 2015, 321) wurde der Beklagten die vorstehend geschilderte Vorgehensweise untersagt. Die Berufungsrichter (OLG Frankfurt/M. MMR 2016, 245) erachteten diese Form der Einholung einer Einwilligung dagegen für zulässig Der BGH setzte das Revisionsverfahren aus und legte dem EuGH Fragen zur Vorabentscheidung vor.

Dies war vor allem die Frage, welche konkreten Anforderungen an eine wirksame Einholung einer Einwilligung zu stellen seien und welche Informationen der Website-Betreiber dem Nutzer diesbezüglich zur Verfügung zu stellen habe.

Die Entscheidung des EuGH:

Maßstäbe der Entscheidung waren sowohl die vormals gültige Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr als auch die Verordnung 2016/679, also die unterdessen geltende DS-GVO selbst.

Der EuGH hat u. a. festgestellt, dass eine wirksame Einwilligung im Sinne der Bestimmungen Art. 2 lit. f. Art. 5 Abs. 3 der Richtlinie 2002/58/EG in Verbindung mit Art. 2 lit. h der Richtlinie 95/46/EG bzw. mit Art. 4 Nr. 11 und

2 EuGH, Urteil vom 01.10.2019, C 673/17.

Art. 6 Abs. 1 lit. a DS-GVO nicht vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies[3] durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss.[4]

Die Einwilligung darf nicht vermutet werden, sondern muss sich aus einem aktiven Verhalten des Nutzers ergeben.[5] Hierfür spricht auch der Erwägungsgrund 32 der DS-GVO wonach Stillschweigen, bereits angekreuzte Kästen oder Untätigkeit der betroffenen Person keine Einwilligung darstellen sollten.[6]

Bei der Speicherung der im Ausgangsverfahren in Rede stehenden Cookies lag eine Verarbeitung personenbezogener Daten vor (Rn. 45, 67). Der EuGH führte jedoch aus, dass Art. 2 lit. F Art. 5 Abs. 3 RL 2002/58/EG, Art. 2 lit. h RL 95/46/EG bzw. Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a DS-GVO nicht unterschiedlich auszulegen seien, und daher der Nutzer vor jedem Eingriff in die im Endgerät eines Nutzers einer Website gespeicherten oder abgerufenen Informationen zu schützen sei, unabhängig davon, ob dabei personenbezogene oder andere Daten betroffen seien.[7]

Ferner sollen Angaben zur Funktionsdauer der Cookies und ob Dritte Zugriff auf die Cookies erhalten können zu den Informationen zählen, die ein Diensteanbieter dem Nutzer einer Website zu geben hat.[8]

Die klaren und umfassenden Informationen müssen den Nutzer in die Lage versetzen, die Tragweite seiner Einwilligung zu begreifen, weiterhin gewährleisten, dass die Einwilligung in voller Kenntnis der Sachlage abgegeben wurde, und schließlich so klar verständlich sein, dass der Nutzer die

---

3 Bei Cookies ist zu unterscheiden zwischen zwingend erforderlichen Cookies, ohne die der jeweilige Online-Service nicht erbracht werden kann, und solchen, die anderen Zwecken dienen, etwa der Nutzeranalyse oder Werbung. Für letztere Kategorie verlangt Art. 5 Abs. 3 der Richtlinie 2002/58/EG die Einwilligung des Internetnutzers. Es ist umstritten, ob der deutsche Gesetzgeber diese Richtlinie in nationales Recht umgesetzt hat, sodass nach dem Wortlaut der §§ TMG (Telemediengesetz) § 12, TMG § 15 TMG in bestimmten Fällen die Möglichkeit eines Widerrufs (sogenanntes „Opt-Out'') genügen könnte (vgl. dazu Rauer/Ettig, ZD 2016, ZD Jahr 2016 Seite 423 ff.). In der Praxis herrscht Unsicherheit, ob und wenn ja, wie ein Website-Betreiber die Einwilligung des Nutzers in das Setzen von Cookies einholen muss, und welche Informationen den Nutzern zur Verfügung gestellt werden müssen. Der EuGH schafft mit seinem Urteil einen ersten Schritt, um Licht ins Dunkel zu bringen, ohne jedoch auf die Frage der Anwendbarkeit des TMG selbst einzugehen.
4 EuGH, Urteil v. 01.10.2019, C-673/17.
5 EuGH, Urteil v. 01.10.2019, C-673/17, Rn 56.
6 EuGH, Urteil v. 01.10.2019, C-673/17, Rn. 62.
7 EuGH, Urteil v. 01.10.2019, C-673/17, Rn. 66.
8 EuGH, Urteil v. 01.10.2019, C-673/17, Rn. 72 ff.

Funktionsweise der verwendeten Cookies verstehen kann (Rn. 74). Ein vorangekreuztes Einwilligungskästchen für Werbezwecke dürfte damit nicht mehr zulässig sein.

Zur Anwendbarkeit von § 15 TMG musste der EuGH keine Stellung beziehen, sodass die ggf. hierzu folgenden Ansichten des BGH abzuwarten bleiben.

Die Herausforderungen für die Praxis dürften zum Einen sein festzustellen, ob die Verarbeitung einwilligungsbedürftig ist oder nicht, und zum Anderen, wie die Umsetzung unter Berücksichtigung der informatorischen Vorgaben zu erfolgen hat.

Ergänzend ist anzumerken, dass funktionale oder „unbedingt erforderliche" Cookies hingegen nach wie vor auch ohne das Abfragen einer Einwilligung gemäß Art 5 Abs. 3 Richtlinie 2002/58/EG möglich sein dürften.[9]

Für die Aufsichtspraxis ergibt sich aus dem Urteil die Herausforderung, bei ihren zu beaufsichtigenden Verantwortlichen auf die Einhaltung der Vorgaben der Datenschutzgesetze weiterhin hinzuwirken und diese in Anbetracht der aktuellen Entscheidung im Rahmen von Screenings der Websites aktiv zu prüfen sowie ggf. nötige Maßnahmen nach Art. 58 DS-GVO zu ergreifen.

## 2.4 Orientierungshilfe für Anbieter von Telemedien

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat im Frühjahr 2019 eine Orientierungshilfe für Anbieter von Telemedien veröffentlicht:

a) Diese Orientierungshilfe setzt sich zunächst mit der Frage auseinander, ob das deutsche Telemediengesetz (TMG) in datenschutzrechtlicher Hinsicht auch nach dem 25.05.2018 noch Gültigkeit beanspruchen kann oder aber durch die Vorgaben der DS-GVO und deren Anwendungsvorrang überlagert wird. Im Weiteren behandelt sie die sich aus der DS-GVO ergebenden

9 Art 5 Abs. 3 Richtlinie 2002/58/EG: Die Mitgliedstaaten stellen sicher, dass die Benutzung elektronischer Kommunikationsnetze für die Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur unter der Bedingung gestattet ist, dass der betreffende Teilnehmer oder Nutzer gemäß der Richtlinie 95/46/EG klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhält und durch den für diese Verarbeitung Verantwortlichen auf das Recht hingewiesen wird, diese Verarbeitung zu verweigern. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen.

Voraussetzungen für eine rechtmäßige Verarbeitung, insbesondere von Daten aus der Nutzung von Telemedienangeboten, und befasst sich eingehend mit Einwilligungen und dem sogenannten Tracking, also der Datenverarbeitungen zur websiteübergreifenden Nachverfolgung von individuellem Verhalten von Nutzern. [10]

Hinsichtlich der Frage einer möglichen Fortgeltung der Datenschutzregeln des TMG, das insbesondere in seinem § 15 in der Vergangenheit häufig eine maßgebliche Rechtsgrundlage für derartige Datenverarbeitungsprozesse bildete, wird die Auffassung vertreten, dass das TMG nach wie vor in all seinen Bestandteilen in Kraft sei. Gleichwohl werden nach richtiger Ansicht die datenschutzrechtlichen Bestimmungen des TMG durch den Anwendungsvorrang der DS-GVO überlagert und haben insoweit ihre Bedeutung verloren.

b) Zudem ist zu bedenken, dass der EuGH in seinem Urteil vom 1. Oktober 2019 in der Rechtssache C 673/17 (vgl. 2.3.2 Planet 49) klargestellt hat, dass eine wirksame Einwilligung des Betroffenen von diesem eine aktive Willensbekundung voraussetzt. Gerade eine solche ist aber im Regelungskonzept des § 15 Abs. 3 TMG nicht vorgesehen. Ohne auf die Argumentation der Orientierungshilfe an dieser Stelle näher eingehen zu wollen, bleibt trotz einiger anderslautender Literaturstimmen doch festzustellen, dass nach dieser EuGH-Entscheidung jedenfalls im Ergebnis vieles für die Richtigkeit der in der Orientierungshilfe vertretenen Ansätze spricht.

c) Im Rahmen der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO sind die Verantwortlichen verpflichtet nachzuweisen, dass jede vorgenommene Verarbeitung personenbezogener Daten rechtmäßig erfolgt. Diese Verpflichtung gilt auch für die Voraussetzungen, die der jeweilige Erlaubnistatbestand voraussetzt.

Für die Verarbeitung personenbezogener Daten durch nicht-öffentliche Verantwortliche bei der Erbringung von Telemediendiensten kommen insbesondere folgende Erlaubnistatbestände in Betracht:

a) Art. 6 Abs. 1 lit. a DS-GVO - Einwilligung

b) Art. 6 Abs. 1 lit. b DS-GVO - Vertrag

c) Art. 6 Abs. 1 lit. f DS-GVO – berechtigte Interessen

---

10 DSK Orientierungshilfe Telemedien v. März 2019, S. 7, vgl. auch Art. 29 Datenschutzgruppe, WP 194 vom 07.06.2012, S. 10; Leitlinie zur Einwilligung, WP 259 v. 28.11.2017, S. 4.

Die DSK ist im Hinblick auf den Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und die Erstellung von Nutzungsprofilen ermöglichen, der Auffassung, dass diese Art der Verarbeitung in aller Regel nicht auf ein berechtigtes Interesse des Verantwortlichen (Art. 6 Abs. 1 lit. f DS-GVO) gestützt werden kann.[11] Daher ist in der Regel eine vorherige wirksame Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) erforderlich, jedenfalls sofern Dienste eines Dritten eingesetzt werden, der die Daten für eigene Zwecke verarbeitet.

Voraussetzungen der Einwilligung:

Eine wirksame Einwilligung liegt vor, wenn die Voraussetzungen des Art. 4 Nr. 11 in Verbindung mit Art. 7 DS-GVO erfüllt sind. Dies setzt eine für den bestimmten Einzelfall erteilte, freiwillige, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder eine sonstige eindeutige bestätigende Handlung voraus, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten ausdrücklich einverstanden ist.

Der Nutzer muss für eine wirksame Einwilligung daher ausreichende Kenntnis über die jeweiligen Datenverarbeitungsvorgänge, über die jeweils einbezogenen Dritten sowie die Möglichkeit einer gesonderten Zustimmung haben.[12]

Ein Opt-Out Verfahren, eine stillschweigende Erklärung oder die bloße Untätigkeit des Nutzers sollen für die erforderliche aktive Handlung gerade nicht ausreichen. Hierfür spricht insbesondere auch Erwägungsgrund 32 der DS-GVO, der Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit nicht als Einwilligung gelten lassen möchte. Der Nutzer muss eine echte freie Wahl haben sich zu entscheiden, damit von einer freiwilligen Einwilligung gesprochen werden kann. [13]

Beim Opt-Out-Verfahren ist für die Erteilung der Einwilligung keine ausdrückliche Bestätigung erforderlich. Vielmehr muss nur bei einer Verweigerung der Einwilligung eine Voreinstellung vom Nutzer bewusst deaktiviert oder abgewählt werden.

Bei einwilligungsbedürftigen Cookies und weiteren Tools sowie ggf. eingesetzten Bannern ist darauf zu achten, dass bereits beim erstmaligen Öffnen einer Website in der Regel eine Übersicht aller einwilligungsbedürftiger Verarbeitungsvorgänge mit Nennung der Akteure und deren Funktion zur Verfügung steht. Auch sollte es die Möglichkeit geben, ein Auswahlmenü zu aktivieren; während der Banner-Anzeige sind alle Skripte, die potenziell

11 Vgl. Anhang I, DSK Orientierungshilfe Telemedien v. März 2019.
12 DSK Orientierungshilfe Telemedien v. März 2019, S. 9.
13 DSK Orientierungshilfe Telemedien v. März 2019, S. 8, 10.

Nutzerdaten erfassen, zu blockieren. Hintergrund ist hierfür, dass die einwilligungsbedürftigen Datenverarbeitungen erst mit aktiver Einwilligung erlaubt sind. Zudem muss die Datenschutzerklärung und das Impressum jederzeit verfügbar sein[14] Es ist weiterhin auf die Möglichkeit des Widerrufs der Einwilligung hinzuweisen.

Ein *Consent Management System* könnte daher für Anbieter zielführend sein, um die Vorgaben zu erfüllen.

Die Möglichkeit, eine Verarbeitung personenbezogener Daten auch auf den Erlaubnistatbestand des Art. 6 Abs. 1 lit. b (Vertrag bzw. vorvertragliches Verhältnis) zu stützen, wird von der DSK zwar erwähnt, wegen ihrer Komplexität aber nicht näher erläutert.

Der Erlaubnistatbestand des Art. 6 Abs. 1 lit f. DS-GVO wird im Gegensatz dazu ausführlich erläutert. Hierfür sei ein detaillierter *Stufentest* vorzunehmen: Zunächst sei das jeweilige berechtigte Interesse zur Datenverarbeitung zu ermitteln, das auf der zweiten Stufe einer Erforderlichkeitsprüfung unterzogen werden müsse; im letzten Schritt der Interessenabwägung dürften schließlich insbesondere die Grundrechte und Grundfreiheiten der Nutzer das berechtigte Interesse des Verantwortlichen nicht überwiegen.

Es ist stets für jede Verarbeitung und für jedes Tool eine konkrete Analyse des Einzelfalls vorzunehmen. Im Rahmen der Interessensabwägung sind insbesondere die vernünftigen Erwartungen betroffener Personen, die Vorhersehbarkeit/Transparenz, beteiligte Akteure und der Umfang der Datenverarbeitung zu berücksichtigen.

**Was muss der Verantwortliche vor einer Datenverarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO tun?**

1. Schritt: Festlegen, was das Interesse und der Zweck der Verarbeitung sind

2. Schritt: Einstufung des Interesses als „berechtigt“:

- Es muss rechtmäßig sein, d. h. im Einklang stehend mit dem EU-Recht und dem mitgliedstaatlichen Recht.

14 DSK Orientierungshilfe Telemedien v. März 2019, S. 9.

- Es sollte hinreichend klar formuliert sein und hinreichend konkret sein, damit es in einer Prüfung der Interessen des Verantwortlichen gegen die Interessen und Grundrechte der betroffenen Person abgewogen werden kann.

- Es handelt sich um ein reales und bestehendes Interesse, d. h. es ist nicht spekulativ.

3. Schritt: Feststellen, ob die Verarbeitung zum Erreichen des verfolgten Interesses erforderlich ist; d. h. überlegen, ob es andere, weniger stark in die Privatsphäre eingreifende Mittel zum Erreichen des genannten Zwecks der Verarbeitung gibt, die dem berechtigten Interesse des für die Verarbeitung der Daten Verantwortlichen entsprechen.

4. Schritt: Abschätzen, ob die Grundrechte oder Interessen der betroffenen Personen höher zu gewichten sind als das Interesse des für die Verarbeitung Verantwortlichen und ggf. Herstellen eines Gleichgewichts der Interessen durch Schutzmaßnahmen.

Der Inhalt der Orientierungshilfe der DSK gibt zwar zunächst nur die Auffassung der staatlichen Datenschutzaufsichtsinstitutionen wieder. Andererseits wird das Papier durch das Urteil des EuGH vom 1.10.2019 (s. 2.3.2 zu Planet 49)[15] in maßgeblichen Aussagen gestützt und insoweit höchstrichterlich bestätigt. In unserer laufenden Aufsichtspraxis können diese Aussagen der Orientierungshilfe daher nicht einfach ignoriert, sondern müssen berücksichtigt werden, zumal wir diese inhaltlich für gut begründet und fachlich fundiert erachten.

Der Medienbeauftragte für den Datenschutz wird daher für die Anbieter der Landeszentrale einen Workshop anbieten, um die in der Orientierungshilfe angesprochenen Fragestellungen zu vertiefen und an konkreten Beispielen zu illustrieren. Dieser Workshop soll den Auftakt einer Reihe bilden, die die Anbieter in Fragen des Mediendatenschutzes beständig weiterbildet und in deren Rahmen aktuelle Themen praxisnah angegangen werden können. Die Orientierungshilfen der DSK liefern hierfür wichtige inhaltliche Grundlagen.

15 EuGH, Urteil v. 01.10.2019, C-673/17.

# 3. Unsere Tätigkeiten

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

## 3.1 Anfragen

### 3.1.1 *One stop shop* bei Tochterunternehmen: Zuständigkeit und Benennungspflicht

Einige der bei der Landeszentrale zugelassenen – insbesondere bundesweiten – Rundfunk- oder Plattformanbieter operieren mit inländischen Tochtergesellschaften, deren Sitz oftmals nicht in Bayern liegen kann. Soweit Datenverarbeitungstätigkeiten dort stattfinden oder dorthin ausgelagert werden, z.B. Kundenakquise, Nutzerverwaltung usw., und nicht ausdrücklich mittels eines Auftragsverarbeitungsverhältnisses nach Art. 28 DS-GVO zwischen Mutter- und Tochtergesellschaft geregelt sind, wirft dies die Frage nach der örtlich und sachlich zutreffenden Datenschutz-Aufsicht auf.

Die Frage zielt insoweit auch auf den Gesichtspunkt des sogenannten *One-Stop-Shop* ab, der prinzipiell für ein Unternehmen die Möglichkeit eröffnet, trotz unterschiedlicher Niederlassungen an unterschiedlichen Orten, die ansonsten ebenso unterschiedliche örtlich zuständige Datenschutzaufsichtsinstitutionen zur Folge hätten, lediglich einen aufsichtlichen Ansprechpartner zu haben. Dieser richtet sich dann nach der Einheit des Unternehmensverbundes, die einheitlich und zentral für den gesamten Unternehmensverbund Fragen des zutreffenden Umgangs mit Datenschutzgesichtspunkten entscheidet.

Als „One-Stop-Shop" wird in der Wirtschaft wie auch in der öffentlichen Verwaltung die Möglichkeit bezeichnet, einen einheitlichen bürokratischen Ansprechpartner zu bestimmen.

Art. 56 Abs. 1 DS-GVO regelt die Frage der Federführung einer von mehreren in Betracht kommenden Aufsichtsbehörden nur bei grenzüberschreitenden Sachverhalten nach dem Maßstab der jeweiligen „Hauptniederlassung", vgl. Art. 4 Nr. 16 DS-GVO). Als europäische Norm gilt diese jedoch nicht unmittelbar für den hier – in der Bundesrepublik – interessierenden Fall der Pluralität von Datenschutzaufsichtsbehörden innerhalb einer föderal strukturierten Staatsorganisation mit jeweils eigenen regional zuständigen Datenschutzaufsichtsbehörden bzw. den Fall einer darüber hinaus auch

noch sektoriellen Differenzierung (hier: Rundfunk). Nach § 40 Abs. 2 BDSG findet jedoch im Bereich der nichtöffentlichen Stellen Art. 4 Nr. 16 DS-GVO mit seiner Definition der „Hauptniederlassung" auch auf den Fall mehrerer inländischer Niederlassungen entsprechende Anwendung. Das mit der DS-GVO eingeführte One-Stop-Shop-Verfahren kann somit auch innerhalb der Bundesrepublik eingesetzt werden.

Unter diesem Blickwinkel leitet sich aufgrund der eindeutigen Vorgaben der DS-GVO mit dem Gebot der Einheitlichkeit der Anwendung der DS-GVO und dem Ziel des *One-Stop-Shop* die federführende, also sachliche und örtliche Aufsichtszuständigkeit des Medienbeauftragten für den Datenschutz für inländische Tochterunternehmen eines bei der Landeszentrale zugelassenen Rundfunkanbieters jedenfalls insoweit her, als diese Tochtergesellschaften unter dem bestimmenden Einfluss der Muttergesellschaft stehen. Werden die Entscheidungen über die Zwecke und die Mittel der Verarbeitung personenbezogener Daten einheitlich durch die Muttergesellschaft getroffen und die jeweils betroffene Tochtergesellschaft hat – unabhängig von ihrem inländischen Sitz – diese Vorgaben stets umzusetzen, besteht die Möglichkeit, für Mutter- und Tochtergesellschaften lediglich eine zuständige Aufsichtsinstitution zu besitzen.

Eine darüber hinausgehende Meldung eines Datenschutzbeauftragten an die am Ort der jeweiligen Niederlassung ansonsten nach Landesrecht vorgesehenen Aufsichtsbehörden ist unter den eben genannten Voraussetzungen nach Ansicht des Mediendatenbeauftragten nicht notwendig. Die Mitteilungspflicht des Art. 37 Abs. 7 DS-GVO beschränkt sich hier unseres Erachtens auf die federführend zuständige Aufsichtsbehörde, also ggf. auch auf den Medienbeauftragten für den Datenschutz bei der BLM.

Gleichwohl sollten die betroffenen Anbieter dann aber die gesamte Bestimmung des Art. 37 Abs. 7 DS-GVO im Blick haben, wonach die Kontaktdaten des Datenschutzbeauftragten nicht nur der – zuständigen – Aufsichtsbehörde mitgeteilt werden, sondern durch den Verantwortlichen oder Auftragsverarbeiter auch veröffentlicht werden müssen. Dadurch wird den Betroffenen sowie den Aufsichtsbehörden ermöglicht, den Ansprechpartner für datenschutzrechtliche Belange direkt zu kontaktieren[16].

16 vgl. hierzu näher Paal/Pauly, Datenschutz-Grundverordnung, DS-GVO Art. 37 Rn. 17; Gola, DS-GVO, Art. 37 Rn. 19.

### 3.1.2 Gestaltung von Datenschutzerklärungen

Die Verpflichtung, bestimmte Informationen in Form einer Datenschutzerklärung vorzuhalten besteht zwar nicht erst seit Inkrafttreten der DS-GVO; dennoch erreichten den Medienbeauftragten für den Datenschutz auch im Berichtszeitraum zahlreiche Anfragen zur gesetzeskonformen Ausgestaltung von Datenschutzerklärungen.

Besonders erwähnenswert war dabei eine Anfrage, bei der ein Dienstleister Textbausteine für die Datenschutzerklärungen seiner Kunden entwickelte, da ihm in bestimmten Bereichen besser bekannt war, welche technischen Vorgänge konkret abliefen und an welchen Stellen personenbezogene Daten verarbeitet wurden. Da diese Textbausteine voraussichtlich bei einem Großteil der bei der BLM zugelassenen Lokal-TV-Angebote eingesetzt werden sollten, unterstützte der Mediendatenbeauftragte die Ausgestaltung beratend.

Ein zentraler Aspekt ist auch bei Datenschutzerklärungen, dass Inhalte auf immer mehr und unterschiedlichen Verbreitungswegen ausgespielt werden. Wenn eine Datenschutzerklärung nicht nur über die Website abrufbar sein soll, sondern auch auf Smart-TV-Geräten oder Streaming-Sticks, kann es vorkommen, dass die Datenschutzerklärung je nach Endgerät unterschiedlich dargestellt wird. Dies kann in Einzelfällen dazu führen, dass Verlinkungen nicht mehr ausgewählt werden können oder vorhandene *Opt-Out*-Schalter nicht mehr ordnungsgemäß funktionieren: sei es, dass die Schalter gänzlich ohne Funktion und nicht mehr bedienbar sind, dass die Bedienung eines Schalters keine Auswirkung auf die dahinterliegenden Funktionen hat oder dass die Darstellung nicht den tatsächlich hinterlegten Einstellungen entspricht. Dies wiederum kann zu Fehlbedienungen führen, z. B. indem eine wiederholte Bedienung statt des erneuten scheinbaren *Opt-Out* vom System als *Opt-In* interpretiert wird. Sofern Pflichtinformationen somit automatisiert über Contentmanagementsysteme auf unterschiedlichen Endgerätekategorien angezeigt werden sollen, empfiehlt es sich, bei der Erstellung bzw. bei Änderungen die tatsächliche Ausgabe zu prüfen.

### 3.1.3 Medienprivileg

Das Datenschutzrecht geht seit jeher und so auch die DS-GVO davon aus, dass die Verarbeitung personenbezogener Daten durch Dritte entweder einer Einwilligung des Betroffenen oder einer Rechtsgrundlage bedarf, die

die konkrete Verarbeitung zu bestimmten, vorher festgelegten Zwecken erlaubt. Diese Zielsetzung kollidiert ebenso seit jeher mit der üblichen Arbeitsweise von Rundfunk und Presse einerseits wie auch mit deren verfassungsrechtlich vorgegebenem und geschütztem Funktionsauftrag andererseits. Da sich die beiden insoweit entgegengesetzten Rechtspositionen jeweils auf verfassungsrechtliche Vorgaben wie auch Grundrechtspositionen berufen können, kann eine Lösung nur in einem wertenden Ausgleich dieser Positionen bestehen.

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

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

Um das daraus sich ergebende oben geschilderte verfassungsrechtliche Dilemma zu lösen, wird den Mitgliedstaaten in Art. 85 Abs. 1 DS-GVO aufgegeben, das Recht auf Schutz der personenbezogenen Daten mit den Vorgaben der Rundfunk- und Pressefreiheit in Einklang zu bringen. Zu diesem Zweck wird den Mitgliedstaaten das Recht eingeräumt, von den meisten Vorgaben der DS-GVO Ausnahmen für die Verarbeitung zu journalistischen Zwecken vorzusehen. Hiervon hat der deutsche Gesetzgeber für den Rundfunk in § 9c RStV[17] einen sehr weitgehenden Gebrauch gemacht.

Zusammengefasst lässt sich feststellen, dass es für die Verarbeitung personenbezogener Daten zu journalistischen Zwecken keiner weiteren darüber hinausgehenden Rechtsgrundlage bedarf, die diese Zwecke verfolgenden

17 Ergänzend ist für die Ausgestaltung des Medienprivilegs Art. 20 Abs. 6 S. 2 BayMG und für den Bereich der Telemedien die §§ 57, 59 RStV, für die Presse Art. 11 BayPrG und im Übrigen Art. 38 BayDSG zu erwähnen.

Personen lediglich das in § 9c RStV niedergelegte Datengeheimnis zu beachten haben und den Betroffenen anstelle der Rechte der DS-GVO lediglich die in § 9c Abs. 2 und 3 RStV genannten Rechte zustehen.

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

Dementsprechend spielt die Frage, ob für bestimmte 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 Fragen des Medienprivilegs, seiner Anwendung und Reichweite zuständig ist, werden immer wieder Fragen von ganz grundlegenden bis hin zu sehr speziellen Ausgestaltungen an ihn herangetragen.

Diese beginnen zumeist mit der Problematik, wer sich auf das so genannte Medienprivileg berufen kann, wofür es letztlich auf die Frage ankommt, welche Ausgestaltung der Gesetzgeber dem Begriff der journalistischen Zwecke beigeben wollte. Ist diese Frage für zahlreiche Angebotsformen des Internets durchaus umstritten und daher häufig nur schwierig zu beantworten, dürfte diese Frage für diejenigen vergleichsweise klar zu entscheiden sein, die Rundfunkprogramme inhaltlich gestalten. Steht dies fest, ist in aller Regel jedenfalls für Datenverarbeitungsprozesse im Zusammenhang mit der inhaltlichen Gestaltung dieser Programme von einer Anwendung des Medienprivilegs auszugehen.

In der Praxis spielten im Berichtszeitraum auch Fragen an den Schnittstellen von Rundfunkgestaltung, Pressetätigkeit und auch kirchlicher Trägerschaft der Herausgeber solcher Angebote eine Rolle.

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

### 3.1.4 Webcam im Studio

Eine auf den ersten Blick relativ einfache Anfrage eines Hörfunkanbieters zeigte, dass auch solche Anfragen oftmals Grenzbereiche zum Medienprivileg ansprechen und weitere tiefgehende Fragen aufwerfen bzw. nach sich ziehen können, die in die künftige Beratung und auch Prüfpraxis eingehen.

Der Anbieter plante, in seinem Sendestudio eine Webcam zu installieren und damit das Geschehen aus dem Studio ins Internet zu übertragen. Zusätzlich sollten Ausschnitte der Übertragung für Beiträge in sozialen Netzwerken verwendet werden.

Daraus ergab sich als erstes die Frage, wo sich diese Übertragung datenschutzrechtlich verorten lässt. Handelt es sich dabei um eine Videoüberwachung am Arbeitsplatz oder ist die Übertragung selbst als journalistisch-redaktionell zu qualifizieren, weshalb sie unter das oben bereits behandelte Medienprivileg (s. 3.1.3) fallen würde? Je nach Einordnung von Umsetzung und Zweck ergeben sich unterschiedliche Rechtsgrundlagen, auf die der Verantwortliche die Verarbeitung stützen kann.

Das Problem einer gegebenenfalls unzulässigen Videoüberwachung kann z. B. dadurch ausgeschlossen werden, dass die Steuerung der Videoaufzeichnung durch die betroffenen Moderatoren selbst erfolgt. Inwieweit es sich bei einer reinen Webcamübertragung aus dem Sendestudio und bei der Verwendung der Ausschnitte für Social Media Beiträge um eine Datenerhebung für journalistische Zwecke handelt, für die das Medienprivileg gelten würde, oder ob eher Marketingaspekte im Vordergrund stehen, ist im jeweiligen Einzelfall zu prüfen.

Grundsätzlich ist es in solchen Fällen sicherlich sinnvoll, Einwilligungen der Betroffenen gemäß Art. 6 Abs. 1 lit. a DS-GVO einzuholen. Dies bezieht sich

nicht nur auf die Mitarbeiter, sondern insbesondere auch auf unregelmäßig im Sendestudio anwesende Personen, wie beispielsweise Studiogäste. Bei Mitarbeitern besteht ggf. auch die Möglichkeit, anstelle einer Einwilligung auf entsprechende vertragliche Vereinbarungen als Rechtsgrundlage zu setzen.

Sowohl bei der Einwilligung als auch bei einer arbeitsvertraglichen Regelung ist darauf zu achten, dass der Betroffene in ausreichendem Maße insbesondere über die gespeicherten Daten und ihre Verwendung informiert wird und die Freiwilligkeit der Erklärungen des Betroffenen nicht durch Kopplungszusammenhänge beeinträchtigt wird.

Die zusätzliche Übertragung von Webcambildern stellt kein ungewöhnliches Merkmal eines Hörfunkangebotes mehr dar; andererseits ist es auch für Hörfunkangebote oftmals für Marketingzwecke von großer Bedeutung, mit Bewegbildinhalten in sozialen Netzwerken präsent zu sein. Daher kann seitens des Anbieters durchaus ein berechtigtes Interesse gemäß Art.6 Abs. 1 lit. f DS-GVO bestehen.

In diesem Fall muss das berechtigte Interesse des Verantwortlichen jedoch mit den Rechten der betroffenen Person abgewogen werden, wobei sicherlich andererseits auch zu berücksichtigen ist, dass mit der Berufswahl als Hörfunkmoderator stets ein gewisses Maß an Öffentlichkeit verbunden ist.

Regelmäßig müssen die betroffenen Personen zudem darüber informiert werden, dass eine Übertragung des Live-Videos auch über Plattformen wie Facebook erfolgen soll und damit die Datenschutzbedingungen der jeweiligen Plattform zum Tragen kommen. So werden Inhalte und damit auch Videoaufzeichnungen nach aktuellem Stand beispielsweise von Facebook nicht gelöscht, sondern lediglich nicht mehr angezeigt. Gleiches gilt für Ausschnitte, die auf anderen Socialmediaplattformen verbreitet werden.

## 3.2 Beschwerden und Kontrollanregungen

Die Anzahl der Beschwerden ist im Vergleich zum letzten Berichtszeitraum weiterhin gestiegen. Zusätzlich dazu wurden deutlich mehr Anfragen von interessierten Bürgern, Websites oder Formulierungen bezüglich des Datenschutzes zu überprüfen, an uns herangetragen. Dies belegt deutlich, dass das Interesse der Bevölkerung an und die Sensibilität für Datenschutzfragen auch im Berichtszeitraum unvermindert zugenommen hat.

### 3.2.1 Auskunftsanspruch

Ein großer Teil der Beschwerden befasste sich zu Beginn des Berichtszeitraums, also seit Ende Mai 2018, mit Auskunftsansprüchen Betroffener über die zu ihrer Person gespeicherten personenbezogenen Daten. Es gab zahlreiche Fälle, in denen Anbieter dieser Verpflichtung nicht innerhalb der vorgesehenen Frist nachgekommen sind.

Nach Art. 12 Abs. 3 Satz 1 DS-GVO müssen „Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags" zur Verfügung gestellt werden. Daher muss eine Auskunft in der Regel unverzüglich – nach nationalem Verständnis ohne schuldhaftes Zögern –, jedenfalls aber innerhalb der Monatsfrist bereitgestellt werden.

Bei den aufgetretenen Fällen wurden die jeweiligen Verantwortlichen aufgefordert, ihren Pflichten fristgemäß nachzukommen. Die Verzögerungen wurden nicht selten mit Personalknappheit begründet. Gleichwohl gilt für die Auskunftserteilung ein unverzüglicher Anspruch auf Auskunft, in jedem Fall aber innerhalb eines Monats. Die Monatsfrist darf in der Regel nur bei komplexen Sachverhalten ausgeschöpft werden, nicht aber bei Standardfällen.[18] Eine eventuell erforderliche Fristverlängerung hat der Verantwortliche auch in jedem Einzelfall zu begründen, Art. 12 Abs. 3 Satz 2, 3 DS-GVO.

Grundsätzlich sollte der Verantwortliche in der Lage sein, einfachgelagerte Auskunftsansprüche unverzüglich zu erfüllen. Pauschale Hinweise in der Eingangsbestätigung an den Auskunftbegehrenden, dass die Auskunftserteilung aufgrund der großen Anzahl von Anfragen noch andauere, und entsprechende Bitten um Geduld im Hinblick auf die Bearbeitung eines Auskunftsverlangens, sahen wir kritisch.

Einmalige, begründete Fristverlängerungen können vorübergehend vorkommen, wenn gehäuft Anfragen auftreten, die auch bei bester Organisation nicht vorhersehbar sind. Eine dauerhafte pauschale Verweisung auf ein großes Anfragevolumen wird wohl kaum ausreichen. Mangelnde organisa-

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

torische Vorkehrungen lassen vielmehr darauf schließen, dass der Verantwortliche seinen technisch organisatorischen Verpflichtungen nicht ordnungsgemäß nachkommt.

Die zunächst langen Bearbeitungszeiten konnten die Verantwortlichen durch entsprechende organisatorische Maßnahmen alsbald in den Griff bekommen und waren letztlich auch dem Umstand geschuldet, dass deutlich mehr Betroffene ihre Rechte wahrgenommen haben, als dies für die Verantwortlichen vorhersehbar war. Die Verantwortlichen wurden auf die verpflichtenden Vorgaben des Art. 12 Abs. 3 DS-GVO gleichwohl hingewiesen.

In allen Fällen wurde der Rechtsanspruch der Betroffenen auf Auskunft im Anschluss, wenn auch gelegentlich erst nach Einschaltung der Aufsicht, erfüllt. Inzwischen gibt es kaum noch an uns herangetragene Beschwerden Betroffener bezüglich nicht rechtzeitig erteilter Auskünfte. So ist davon auszugehen, dass sich das Vorgehen der Verantwortlichen eingespielt hat und Auskünfte nun umgehend erteilt werden.

In unserer Praxis sind die uns zur Kenntnis gelangten Auskunftsanfragen in der Regel umfassend beantwortet worden. Grundsätzlich sollte die Auskunft so umfassend sein, dass der Betroffene den Umfang und Inhalt seiner gespeicherten personenbezogener Daten beurteilen kann. Davon nicht erfasst sind in der Regel interne Dokumente des Verantwortlichen bzw. sämtlicher geführter Schriftverkehr, der dem Betroffenen bereits bekannt ist.[19]

### 3.2.2 Datenlöschung

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

In der Mehrzahl dieser Fälle konnte der Medienbeauftragte für den Datenschutz jedoch feststellen, dass ein Verstoß gegen datenschutzrechtliche Vorgaben der DS-GVO nicht vorlag: Art. 17 Abs. 1 lit. a der DS-GVO sieht zwar eine Löschverpflichtung des Verantwortlichen vor, wenn eine weitere Verarbeitung der Daten der betroffenen Person für den ursprünglichen

19 AG München, Teilurteil v. 04.09.2019, 155 C 1510/18, Rn. 21

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. 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.

Diese Vorschriften stellen eine rechtliche Verpflichtung im Sinne des Art. 17 Abs. 3 lit. b DS-GVO dar, sodass in einem solchen Fall trotz der grundsätzlichen Löschverpflichtung tatsächlich die Löschung erst nach Ablauf der in der Regel mehrjährigen Aufbewahrungspflichten erfolgen kann. Diese für zahlreiche Petenten überraschende Rechtslage ließ sich häufig erst nach Einschaltung der Aufsicht vermitteln, wobei auch auf Seiten der Verantwortlichen gelegentlich eine umfassendere Information der Betroffenen hilfreich wäre.

### 3.2.3 Einwilligung und Gewinnspiel: Rechenschaftspflicht

Im Laufe des Berichtszeitraum kam es zu einigen Beschwerden über Telefonanrufe nach der Teilnahme an Gewinnspielen, wobei die Betroffenen vortrugen, jedenfalls keine Einwilligungserklärung in künftige werbliche Telefonanrufe abgegeben zu haben.

In der überwiegenden Anzahl der Fälle stellte sich jedoch heraus, dass die Gewinnspielteilnehmer wohl doch darüber informiert waren, dass das gewinnspielausführende Unternehmen die Daten zu schriftlichen und telefonischen Werbezwecken auch an namentlich genannte Kooperationspartner weiterleiten werde. Diese Information war häufig bereits in der Einwilligungserklärung zum Gewinnspiel in einfach verständlicher Sprache angegeben und musste mittels eines Ankreuzkästchens auch aktiv angekreuzt werden. Dies war in den uns vorgelegten Fällen auch so geschehen, sodass insofern keine Datenschutzverstöße festgestellt werden konnten. Gleiches galt in der Regel für den Hinweis auf das jederzeitige Widerrufsrecht.

In diesen Fällen wurden uns Nachweise dafür vorgelegt, dass die jeweiligen Einwilligungen auch tatsächlich abgegeben worden wären. Insoweit war davon auszugehen, dass die Verantwortlichen ihrer Rechenschaftspflicht gemäß Art. 5 Abs. 1 lit. a, Abs. 2, Art. 24 Abs. 1 DS-GVO nachgekommen waren.

Auch nach der Rechtsprechung des BGH ist beim Nachweis des Einverständnisses bei Werbeanrufen erforderlich, dass der Werbende die konkrete Einverständniserklärung jedes einzelnen Verbrauchers vollständig dokumentiert, was im Fall einer elektronisch übermittelten Einverständniserklärung deren Speicherung und die jederzeitige Möglichkeit eines Ausdrucks voraussetzt.[20] Die Rechtsprechung hat inzwischen entschieden, dass es zulässig sei, die Teilnahme an einem Gewinnspiel davon abhängig zu machen, dass die Einwilligung in künftige Werbung durch acht konkret bezeichnete Unternehmen erteilt wird. Dabei muss jedoch der Geschäftsbereich der werbenden Unternehmen hinreichend klar beschrieben sein.[21]

### 3.2.4 Werbung trotz Widerrufs

Häufig erreichten uns Beschwerden, weil die Betroffenen von Ihnen als unerfreulich empfundenen Zusendungen wie z. B. Newsletter erhalten hatten, obwohl die betroffenen Personen jeweils ihre Einwilligung für den Versand gemäß Art. 7 Abs. 3 DS-GVO widerrufen hatten. In zahlreichen Fällen war ihnen hierüber sogar eine Bestätigung zugegangen.

Die Verantwortlichen begründeten diesen Fehler häufig mit der Aussage, dass der Widerruf aufgrund der Vielzahl an eingegangen Anfragen nicht schnell genug bearbeitet und entsprechend vermerkt worden sei. In einigen Fällen war menschliches Versagen die Ursache, da Mitarbeiter schlicht die Anfrage nicht an die zuständige Abteilung weitergeleitet hatten.

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

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

---

20 BGH, Urteil v. 10.02.2011, I ZR 164/09 Rn. 31.
21 OLG Frankfurt a.M., Urteil v. 27.06.2019, 6 U 6/19.

### 3.2.5 Passwortsicherheit

Einige Beschwerden des Berichtszeitraumes betrafen das Thema Passwortsicherheit und hierbei überwiegend Zugangsschranken zu Kundenbereichen auf Websites, die durch ein Passwort oder einen PIN-Code geschützt waren. Sofern in Kundenbereichen auch sensible personenbezogene Daten abrufbar sind, stellte sich in solchen Fällen häufig die Frage, welche Anforderungen im Einzelfall an ein Passwort zu stellen sind.

Innerhalb der technischen Umgebung haben Unternehmen einen gewissen Spielraum, wie sie Sicherheitsfragen ausgestalten und z. B. mit dem Einrichten von Passwörtern umgehen.

Gibt ein Anbieter ein bestimmtes Verfahren vor, so hat dieses in einem angemessenen Verhältnis zu den dahinter verfügbaren Kundendaten zu stehen. Wird z.B. aus Gründen der Kundenakzeptanz lediglich ein vierstelliger PIN-Code eingesetzt, kann je nach Sachlage eine Kombination mit weiteren Faktoren erforderlich sein. Erfordert der Login-Vorgang zusätzlich eine Kundennummer oder eine E-Mailadresse, entsteht ein deutlich höheres Sicherheitsniveau.

Wird nach drei gescheiterten Login-Versuchen das Benutzerkonto ganz oder zeitweise gesperrt, kann auch ein lediglich vierstelliger PIN Code eine akzeptable Schranke darstellen. Diese lässt sich nochmals erhöhen, wenn technische Vorkehrungen eingesetzt werden, die eine automatische Wiederholung der PIN-Eingabe verhindern. Die ohne derartige Zusatzvorkehrungen nachvollziehbaren Bedenken im Hinblick auf das mögliche Erraten einer vierstelligen PIN lassen sich auf diese Weise entkräften.

Andererseits sind bei der Ausgestaltung technischer Sicherungsmaßnahmen zahlreiche Gesichtspunkte zu berücksichtigen und in einen Ausgleich zu bringen: Art, Umfang, Umstände wie auch Zwecke der Datenverarbeitung, die unterschiedlichen Eintrittswahrscheinlichkeiten und die Implementierungskosten. Daher besitzen die Verantwortlichen bei der Gestaltung der technischen Sicherungsmaßnahmen eine gewisse Einschätzungsprärogative, die auch Fragen der Akzeptanz der Maßnahmen beim Kunden und Ähnliches berücksichtigen kann. Anforderungen an ein Passwort und andere Sicherungsmaßnahmen sind dabei immer in Zusammenhang mit dem jeweiligen Einsatzzweck zu betrachten.

Grundsätzlich gibt es zahlreiche Möglichkeiten, die Passwortsicherheit zu erhöhen und unberechtigte Zugriffe zu verhindern. Es wäre beispielsweise empfehlenswert, die Nutzer zur Vergabe längerer Passwörter aufzufordern oder es ihnen zumindest zu ermöglichen und die dabei verwendbaren Zeichen nicht nur auf Ziffern zu beschränken. Dabei können auch Vorkehrungen getroffen werden, die die Vergabe von schwachen Passwörtern verhindern. Denkbar wäre z. B. eine Prüfung hinsichtlich der Komplexität des Passworts und eine Anzeige sowie Bewertung der Passwortstärke. Auch die Vorgabe einer Mindeststärke erscheint sinnvoll, um Trivialpasswörter zu verhindern.

Wenn der Nutzer über Änderungen an seinen Zugangsdaten oder seinem Nutzerprofil per E-Mail informiert wird, verringert sich das Risiko, dass Unbefugte, sofern sie Zugang zum Kundenkonto erlangen konnten, darin Änderungen vornehmen können – ohne dass dies vom Betroffenen wahrgenommen wird. Ebenso können auch fehlgeschlagene Loginversuche dem Nutzer mitgeteilt werden. Um *Brute-Force-Attacken*, bei denen ein Passwort automatisiert durch Ausprobieren geknackt wird, zu verhindern, ist es zielführend, den Zugang nach wenigen Fehlversuchen dauerhaft oder zumindest für eine bestimmte Zeitspanne zu sperren.

Um ein vergessenes Passwort zurückzusetzen, ist es in jedem Fall erforderlich, auf Informationen zurückzugreifen, die eine Identifikation des jeweiligen Nutzers voraussetzen. So kann beispielsweise ein entsprechender Link an die ursprünglich im System hinterlegte E-Mail-Adresse gesendet werden.

Eine erhebliche höhere Sicherheit lässt sich durch den Einsatz einer *Zwei-Faktor-Authentifizierung (2FA)* bzw. *Multi-Faktor-Authentifizierung (MFA)* erreichen. Dabei wird die Zugangsberechtigung durch zwei oder mehr unabhängige Faktoren überprüft. Neben den üblichen Zugangsdaten wird hier beispielsweise ein SMS-Code oder ein App-Token eingesetzt, wodurch auch die meisten Phishing-Attacken verhindert werden können.

Die Abwägung dieser und ähnlicher Gesichtspunkte war im Rahmen der im Berichtszeitraum auf der Grundlage von Beschwerden zu beurteilenden Fallgestaltungen durchzuführen.

Was ist Multi-Faktor-Authentifizierung? Als Multi-Faktor-Authentifizierung wird der Vorgang bezeichnet, die Identität eines Nutzers anhand mehrerer voneinander unabhängiger Faktoren zu überprüfen. Bekannte Beispiele in der Praxis sind biometrische Merkmale wie Fingerabdrücke, TAN-Generatoren, Chipkarten oder andere Hardwareschlüssel, die als zusätzliche Faktoren neben einem Passwort verwendet werden.

### 3.2.6 Verschlüsselung von Daten

Direkten Bezug zum Bereich Passwortsicherheit hat das Thema Verschlüsselung. In Art. 32. Abs. 1 lit. a DS-GVO wird Verschlüsselung explizit als eine

mögliche Maßnahme genannt, um bei der Verarbeitung von personenbezogenen Daten ein angemessenes Schutzniveau zu gewährleisten. Dies kann sowohl für die Speicherung von Daten als auch für deren Übertragung relevant sein.

Im Berichtszeitraum war im Rahmen von Beschwerden zu diesem Themenkomplex zu prüfen, ob Übertragungsvorgänge von Login-Daten wegen einer fehlenden Transportverschlüsselung unzureichend gesichert wären. In den zu prüfenden Fallgestaltungen konnten die Bedenken der Beschwerdeführer ausgeräumt werden. Es gab zwar im Rahmen des Login-Prozesses einzelne unverschlüsselte Datenverbindungen. Die Übertagung der Zugangsdaten selbst fand jedoch jeweils verschlüsselt statt.

Grundsätzlich ist insbesondere bei der Übertragung von personenbezogenen Daten, wie beispielsweise bei Kontaktformularen auf eine ausreichende Transportverschlüsselung zu achten, sodass die HTTPS-Konfiguration von Websites dem Stand der Technik entspricht. Das bedeutet beispielsweise, dass möglichst keine veralteten und damit unsicheren Verschlüsselungsprotokolle verwendet werden. So sollten mindestens die TLS-Version 1.2 sowie geeignete Zertifikate mit ausreichenden Schlüssellängen eingesetzt werden.

Auch bei der Übertragung von E-Mails ist auf eine hinreichende Transportverschlüsselung zu achten. Sofern bei den übermittelten Inhalten ein erhöhtes Risiko anzunehmen ist oder die Kommunikationspartner selbst einer Risikogruppe angehören, sollte eine Inhaltsverschlüsselung genutzt werden. In diesem Zusammenhang ist es angebracht, dass Unternehmen die Möglichkeit der inhaltsverschlüsselten Kontaktaufnahme zumindest anbieten, auch wenn diese in den meisten Fällen nicht erforderlich sein mag und nur selten genutzt wird.

Auch wenn keine Übertragung über das Internet stattfindet, kann die Verschlüsselung von Daten erforderlich sein. So waren im Berichtszeitraum Fragen im Zusammenhang mit auf dem Postweg verloren gegangenen USB-Sticks mit personenbezogenen Daten zu prüfen und auf ihre Folgen zu untersuchen. Sind die Daten jedoch dem Stand der Technik entsprechend wirksam verschlüsselt und mit einem ausreichend langen Passwort versehen, ist das Risiko für die Rechte und Freiheiten des Betroffenen in der Regel als eher gering einzuschätzen.

### 3.2.7 Tracking Tools

Im Berichtszeitraum erreichten den Mediendatenbeauftragten mehrere Beschwerden hinsichtlich der auf Websites eingesetzten *Trackingtools*. In den darauffolgenden Prüfverfahren wurden neben dem Tracking an sich auch die Information der Nutzer über die Datenerhebung und die Gestaltung der – soweit vorhanden – Einwilligungserklärungen einer genaueren Betrachtung unterzogen.

Eine Stichprobenuntersuchung bei verschiedenen bayerischen Rundfunkanbietern ergab, dass sich viele bereits der Thematik angenommen haben, jedoch weiterhin noch großer Handlungsbedarf besteht. Ursprünglich war geplant, im ersten Halbjahr 2020 hierzu eine Informationsveranstaltung für die Verantwortlichen im Zuständigkeitsbereich des Mediendatenbeauftragten durchzuführen. Diese wird in geeigneter Form nachgeholt werden, sobald Sie wieder sinnvoll durchführbar erscheint.

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

Bei der Einbindung eben dieser Drittanbieter, die die Nutzungsdaten auch für eigene Zwecke nutzen und bei denen es sich somit nicht um ein reines Auftragsverarbeitungsverhältnis handelt, ist genau zu prüfen, ob eine Einwilligung des Nutzers erforderlich ist und ob diese im konkreten Fall auf der Grundlage hinreichender Informationen erteilt wurde.

Bislang wurden die Anbieter lediglich auf aus unserer Sicht datenschutzrechtlich problematische Aspekte ihrer Websites hingewiesen und ihnen die Möglichkeit gegeben, ihre Angebote entsprechend anzupassen. Künftig wird es auch in diesem Bereich zu intensiveren Prüfungen und Bewertungen kommen müssen, die gegebenenfalls auch aufsichtliche Maßnahmen nach sich ziehen können.

In diesem Zusammenhang sei nochmals auf die Orientierungshilfe für Telemedienanbieter (vgl. oben unter 2.4) hingewiesen der sich der Medienbeauftragte für den Datenschutz inhaltlich angeschlossen hat.

Was ist Browserfingerprinting? Fingerprinting ist eine Methode, um Internetnutzer eindeutig wieder erkennen zu können. Dabei wird mittels verschiedener Parameter des jeweilgen Endgeräts eine ID berechnet. Diese ID dient dann als Grundlage für weiteres Tracking. Im Gegensatz zu Cookies ist ein Löschen der ID bzw. des Fingerprints nicht möglich. Fingerprinting lässt sich nur dadurch unterbinden, indem durch Zusatzprogramme den Berechnungen Zufallswerte beigeführt werden, wodurch die Endgeräte nicht mehr wiedererkannt werden.

### 3.2.8 Datenweitergabe an Inkassobüros

Auch in diesem Berichtszeitraum bemängelten einige Beschwerdeführer, dass ihre Daten unrechtmäßig an ein Inkassobüro weitergegeben worden seien.

Beim überwiegenden Teil dieser Beschwerden konnte festgestellt werden, dass den Übermittlungen tatsächliche Forderungen zugrunde lagen und diese Übermittlungen daher zumeist rechtmäßig erfolgten. Die zivilrechtliche Prüfung des Bestehens der maßgeblichen Forderungen stellt dabei eine inzident zu entscheidende Vorfrage dar, bei welcher den Parteien der ordentliche Rechtsweg offensteht. Liegt in diesem eine Entscheidung vor, wird diese vom Mediendatenbeauftragten übernommen.

Besteht danach eine Forderung, steht es dem Verantwortlichen frei, sich eines Inkassobüros zu bedienen, dem die für seine Tätigkeit erforderlichen Informationen zur Verfügung gestellt werden dürfen. Ein Widerspruchsrecht, wie es gelegentlich von Beschwerdeführern angenommen wird, besteht gegen eine solcherlei rechtmäßige Weitergabe nach den Vorgaben der DS-GVO nicht.

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

## 3.3 Datenpannen

### 3.3.1 Allgemeines zu Artikel 33 DS-GVO

Die DS-GVO verlangt u. a., dass personenbezogene Daten mithilfe geeigneter technischer und organisatorischer Maßnahmen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, sodass die Daten, ob unbeabsichtigt oder unrechtmäßig, vor Vernichtung, Verlust, Veränderung oder unbefugtem Zugang bzw. Offenle-

gung geschützt werden.[22] Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn die Sicherheit durch das Kompromittieren von Schutzmaßnahmen verletzt wird.

Schutzziele sind dabei die Vertraulichkeit, die Verfügbarkeit und die Integrität von personenbezogenen Daten.[23] Sobald dem Verantwortlichen eine solche Verletzung 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. Der Verantwortliche ist verpflichtet, jedem ersten Hinweis nachzugehen und zu ermitteln, ob tatsächlich eine Datenschutzverletzung vorliegt.[24]

Datenpannen bilden einen erheblichen Teil unserer täglichen Arbeit und nehmen viel Zeit in Anspruch, da stets der Einzelfall, die betroffenen Daten und die Umstände, die dazu führten, untersucht werden müssen.

### 3.3.2 Fehlversand

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

Die gemeldeten Datenpannen unterschieden sich hinsichtlich der betroffenen und fehlgeleiteten Unterlagen bzw. Informationen, aber auch hinsichtlich der der jeweiligen Panne zu Grunde liegenden Begebenheiten und Ursachen im Vorfeld. Neben technischen und individuellen Fehlern Einzelner mit unterschiedlicher Ausrichtung sind gewisse Ursachenreihen einerseits in der fälschlichen Angabe von Kontaktdaten durch die Betroffenen selbst oder der fehlerhaften Übernahme unzutreffender Kontaktdaten wie z. B. E-Mail-Adressen durch Mitarbeiter von Verantwortlichen aufgetreten. Hinsichtlich der fehlgeleiteten Inhalte läuft das Spektrum von vergleichsweise

22 Vgl. Art. 32, 4 Nr. 12, 33 DS-GVO ; Workingpaper 250 (WP250): Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 v. 06.02.2018 der Art. 29 Datenschutzgruppe, S. 7.
23 WP 250 der Art 29 Datenschutz-Gruppe, S. 8.
24 WP 250 der Art 29 Datenschutz-Gruppe, S. 14.

unbedeutenden Unterlagen wie Newslettern, denen aber dennoch personenbezogene Daten zu entnehmen waren, bis hin zu persönlichen Vertragsunterlagen mit Hinweisen auf Bank- und Kreditkartendaten.

Festzustellen ist, dass die Meldung von Fehlversendungen im Vergleich zum vorherigen Berichtszeitraum erheblich gestiegen ist; alleine im Jahr 2019 waren 48 derartige Vorgänge zu verzeichnen und eine entsprechende Anzahl von Verfahren einzuleiten und durchzuführen.

Die Meldungen erfolgten größtenteils innerhalb der gesetzlichen Vorgaben, sodass nur in einigen wenigen Fällen ergänzende Hinweise erteilt werden mussten. Das Risiko für die Betroffenen war größtenteils nicht hoch, sodass auch in den Fällen einer verspäteten Meldung keine weiteren Maßnahmen ergriffen werden mussten.

Andererseits mussten aber in zwei Fällen umfassende Nachforschungen im Verwaltungsverfahren eingeleitet werden, da mehrere Datensätze und Personen betroffen waren. Diese Verfahren konnten im Berichtszeitraum noch nicht abgeschlossen werden und dauern daher noch an.

### 3.3.3 Verlust von Datenträgern

Im Berichtszeitraum stellte sich auch häufig die Frage, wie mit verlorenen USB Sticks oder mit einem abhanden gekommenen Diensthandy zu verfahren sei.

In allen uns gemeldeten Fällen waren die Datenträger ausreichend verschlüsselt, sodass auf Fragen der einfachen Zugänglichkeit von Daten nicht in besonderem Maße einzugehen war. Festzustellen bleibt, dass Datenträger, auf denen personenbezogene Daten gespeichert sind, stets verschlüsselt sein sollten, damit im Falle eines Diebstahls oder Verlusts ein Schutz vor allzu leichtem unbefugtem Zugriff auf die Daten besteht.

Auch wenn der jeweilige Verantwortliche im Einzelfall aufgrund einer Verschlüsselung ggf. keine Verletzung oder kein Risiko für Rechtspositionen Dritter zu erkennen vermag, erachten wir es gleichwohl für sinnvoll, wenn sich der Verantwortliche beim Verlust auch verschlüsselter Datenträger an die Aufsichtsbehörde wendet, um sich mit dieser abzustimmen. So wird der Aufsicht die Möglichkeit gegeben, die Details des Falles selbst einer Würdigung zu unterziehen, da ihr auch entsprechend Art. 34 Abs. 4 DS-GVO die

letzte Entscheidung darüber gebührt, die eingesetzte Verschlüsselung[25] und ggf. auch deren Schutzstandard zu bewerten.

### 3.3.4 Offener Mailverteiler

Eine weitere Spielart von Datenpannen stellen offene E-Mail Verteiler dar. In diesen werden mehreren oder allen Empfängern einer E-Mail auch die übrigen Adressaten und deren E-Mail-Adressen offenbart, obwohl hierfür keine Rechtsgrundlage besteht.

Wenn diesbezüglich keine Einwilligung der Empfänger zur Offenlegung ihrer Daten oder eine andere Rechtsgrundlage vorliegt, ist die Verwendung eines offenen E-Mail-Verteilers in aller Regel datenschutzrechtlich nicht zulässig.

Auch wenn zumeist der zu erwartende Schaden für die Betroffenen ein begrenzter sein wird, ist das jeweilige Schadenspotenzial dennoch zu ermitteln und sind die gesetzlich vorgesehenen Folgerungen daraus zu ziehen. Treten keine besonderen Umstände hinzu, werden in aller Regel keine Benachrichtigung der Betroffenen erforderlich und organisatorisch über eine nochmalige Sensibilisierung der Mitarbeiter hinaus keine weiteren Maßnahmen veranlasst sein.

25 Vgl. Frank, in Schwartmann/Jaspers/Thüsing, Kugelmann, DS-GVO, 2018, Art. 33 Rn. 38.

### 3.3.5 Phishing-Angriffe und *Emotet* Trojaner

Im Berichtszeitraum wurden zwei in ihrer Struktur ähnliche Fälle gemeldet, in denen Angreifer von außen mit einem gewissen Erfolg versuchten, sich Zugang bzw. die Herrschaft über Datenverarbeitungssysteme von Anbietern zu verschaffen.

Von einem Anbieter wurde gemeldet, dass er Opfer eines Phishing-Angriffs mit internationaler Verbreitung geworden war. Dabei wurden E-Mails über dienstliche E-Mailadressen von Mitarbeitern des Anbieters im größeren Stile verschickt, die die Adressaten dazu verleiten sollten, ihre Zugangsdaten auf einer vermeintlich dem Anbieter zugehörigen Website einzugeben.

In einem uns mitgeteilten Fall führten diese Versuche zum Erfolg. Im Nachgang zu diesem Vorgang schöpfte der betroffene Mitarbeiter jedoch Verdacht und änderte selbstständig sein Passwort.

Da es sich bei der erbeuteten und kurzfristig funktionsfähigen Benutzername-Passwort-Kombination um Zugangsdaten für Systeme handelte, auf die nur im internen Netzwerk des Anbieters zugegriffen werden konnte, waren diese Daten für externe nicht nutzbar. Auch weitere Sachverhaltsrecherchen haben keine weiterführenden datenschutzrechtlichen Risiken ergeben.

Der Anbieter hat direkt nach Bekanntwerden des Angriffs seine Mitarbeiter informiert und über technische Maßnahmen sowohl die weitere Verbreitung der Phishing-Mails als auch den Zugriff auf die korrespondierende Website unterbunden.

Durch das rasche Handeln des Mitarbeiters und des Anbieters konnte ein möglicher Schaden verhindert werden. Datenschutzrechtliche Maßnahmen waren nicht erforderlich.

Ein weiterer Anbieter meldete im Berichtszeitraum einen melde- und benachrichtigungspflichtigen Datenvorfall – verursacht durch einen bis dahin unbekannten *Emotet* Trojaner.

Der *Emotet* Trojaner konnte sich durch das Öffnen eines per E-Mail verschickten infizierten Worddokuments Zugang zum Rechner verschaffen. Er las die Kontaktbeziehungen und E-Mail-Inhalte aus dem betroffenen E-Mail-Postfach sowie einem weiteren Postfach aus. Alle so gefundenen Informationen wurden sodann zur weiteren Verbreitung des Schadprogramms verwendet, indem Empfänger E-Mails mit authentisch aussehenden, jedoch erfundenen Inhalten von Absendern, mit denen sie erst kürzlich in Kontakt

standen, erhielten. Für die Empfänger wirkten die E-Mails wegen der korrekten Angabe von Namen, Mailadresse und Absender sowie auch der Anrede und Signatur authentisch. In der Regel sind diesen E-Mails Links oder Anhänge beigefügt, die Schadsoftware enthalten. Wegen der vermeintlichen Echtheit verleiten die E-Mails auch zum unbedachten Öffnen des schädlichen Dateianhangs oder des in der Nachricht enthaltenen Links. Ist ein Computer erst infiziert, lädt *Emotet* normalerweise weitere Schadsoftware nach. Diese Schadprogramme führen dann oft zu Datenabflüssen oder können den Angreifern auch die vollständige Kontrolle über das betroffene System ermöglichen.

Im uns gemeldeten Fall waren zwei E-Mail-Postfächer infiziert und ausgelesen worden. Der Versuch, weitere Schadsoftware nachzuladen, wurde durch ein Antivirenprogramm verhindert. Der Trojaner wurde innerhalb kurzer Zeit entdeckt, der zunächst infizierte PC isoliert und alle Programme und Software der anderen PCs überprüft. Sofort mit Entdecken des Trojaners wurden alle Personen, die im Postfach aufzufinden waren, sei es durch Kontaktlisten oder E-Mails, in Kenntnis gesetzt, sodass sich der Trojaner nicht weiterverbreiten konnte.

Das betroffene Unternehmen hat aus unserer Sicht korrekt gehandelt und die Vorgaben zur Meldung eingehalten, sodass nach unserer Auffassung keine weiteren datenschutzrechtlichen Maßnahmen erforderlich waren.

Aufgrund der Gefahrenlage von Emotet Angriffen, vgl. auch die Pressemitteilung des BayLDA, sollten die Mitarbeiter stets für derartige datenschutzrechtliche Problemlagen sensibilisiert werden.

Pressemitteilung des BayLDA zur Emotet-Infektionswelle:

https://www.lda.bayern.de/media/pm/pm2019_15.pdf (Download am 20.12.2019)

## 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 Art. 20 BayMG über alle in Art. 58 Abs. 1 bis 5 DS-GVO genannten Befugnisse zur Überwachung und Durchsetzung der Vorgaben der DS-GVO. Dieser umfangreiche Katalog an Befugnissen reicht von den Untersuchungsbefugnissen des Art. 58 Abs. 1 DS-GVO über konkrete Abhilfebefugnisse des Art. 58 Abs. 2 DS-GVO (umfassend die präventive

Warnung, die repressive Verwarnung sowie konkrete Anweisungsbefugnisse) bis hin zur Sanktion der Verhängung von Geldbußen nach Art. 83 DS-GVO als „schärfstes Schwert" der nach der DS-GVO vorgesehenen Maßnahmen. Ein Großteil dieser Maßnahmen kann nicht nur gegenüber dem Verantwortlichen, sondern auch gegenüber Auftragsverarbeitern verhängt werden.

Analog zur Praxis der meisten Aufsichtsbehörden in Deutschland hat sich auch der Medienbeauftragte für den Datenschutz seit Inkrafttreten der DS-GVO zunächst und im Schwerpunkt auf seinen Beratungsauftrag konzentriert und von konkreten Abhilfebefugnissen bisher nur zurückhaltend Gebrauch gemacht. Im Dialog mit den seiner Aufsicht unterstehenden Stellen, insbesondere mit den Anbietern und der BLM, hat er auf eine DS-GVO-konforme Umsetzung datenschutzrelevanter Vorgänge hingewirkt und gelegentlich auch gedrängt.

Soweit auf Beschwerden Betroffener hin Datenschutzverstöße im Raum standen, wurden insbesondere ab der zweiten Jahreshälfte 2019 zur Vorbereitung von Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO Anhörungen in Verwaltungsverfahren gegenüber Verantwortlichen und Auftragsverarbeitern durchgeführt. Aufgrund der Komplexität einiger Vorgänge konnten diese Fälle im Berichtszeitraum noch nicht in Bescheidsform abgeschlossen werden.

Uns vorgetragene Beschwerden, Kontrollanregungen und Datenpannen wurden eingehend geprüft und führten häufig zur Einleitung von eigenständigen Verwaltungsverfahren, was zumeist einen nicht unerheblichen zeitlichen Aufwand mit sich bringt.

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

Bei einigen Fällen erschien es notwendig, die Verantwortlichen auf ein datenschutzkonformes Verhalten hingewiesen und sie anzuhalten, ihre technisch-organisatorischen Maßnahmen zu prüfen und in Einzelfällen nachzubessern.

Im einem grundlegenden Verfahren musste nach einer umfangreichen Sachverhaltsermittlung in einen unmittelbaren mehrstufigen Austausch

mit dem Anbieter eingetreten werden, um komplexe tatsächliche und rechtliche Fragestellungen zu erörtern und eine datenschutzkonforme Gestaltung abzustimmen. Insoweit berührt in derartigen Fällen die Überwachungsfunktion der Aufsichtsbehörden ihre weitere Aufgabe, die ihrer Aufsicht unterliegenden Institutionen auch für die Ihnen aus dem Datenschutzrecht entstehenden Pflichten zu sensibilisieren und dabei auch zu beraten.

## 3.5 Informationen für Anbieter

### 3.5.1 Beratung

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

Diese Aufgabe zu sensibilisieren erstreckt sich vor allem auch auf eine Beratungsfunktion, die bis zur Begutachtung umfassender Datenschutzkonzepte gegebenenfalls sogar von Geschäftsmodellen gehen kann[26] (vgl. 3.4). Das Gesetz verwendet zur Umschreibung der Aufgabe das Wort „sensibilisieren" und gibt dieser Tätigkeit eine gewisse Zielrichtung dahin vor[27], dass die Beratung der Rechtstreue und damit der Einhaltung der Vorgaben des Datenschutzrechtes zu dienen habe.

Die Beratungstätigkeit bezog sich gleichermaßen auf die Landeszentrale einerseits und die Anbieter andererseits, wenngleich dabei hinsichtlich der berührten Themen durchaus Unterschiede aber auch gewisse Überschneidungen erkennbar sind.

Die inhaltlichen Schwerpunkte beginnen bei Zuständigkeitsfragen, die im Bereich des Rundfunkdatenschutzes zusätzliche Schwierigkeiten dadurch aufweisen, dass hier unterschiedliche Organisationsprinzipien aufeinandertreffen, die jedenfalls im Moment noch nicht oder allenfalls rudimentär aufeinander abgestimmt sind. Mit dem Medienstaatsvertrag mag künftig insoweit eine gewisse Klärung und damit auch Verbesserung eintreten. Aber

26 Auernhammer/von Lewinsky § 57 Rn. 16 ff.
27 Auernhammer/von Lewinsky § 57 Rn. 17.

auch die Zuständigkeit für OWi-Verfahren bildete im Hinblick auf die EU Richtlinie RL 2016/680 ein wiederkehrendes Thema.

Eine gewisse Ähnlichkeit hierzu weisen die Fragen auf, die sich um den Umgang mit Organen juristischer Personen und ähnlichen Institutionen wie dem Personal- bzw. Betriebsrat und der insoweit zutreffenden datenschutzrechtlichen Einordnung ranken. Auch in dieser Hinsicht erwachsen aus der Verbindung zum Rundfunkrecht und seinen in gewisser Weise außergewöhnlichen und gelegentlich einzigartigen Gestaltungsformen zusätzliche Herausforderungen.

Ein laufend wiederkehrendes Thema bilden Fragen um die Abfassung und Gestaltung von Datenschutzerklärungen, die zumeist in einem näheren oder ferneren Zusammenhang mit dem Einsatz von Cookies und Tracking-Mechanismen stehen und aufgrund des technischen Fortschritts aber auch dem der Rechtswissenschaft und hierbei insbesondere aufgrund der Entwicklung der Rechtsprechung einem stetigen Fortschritt oder jedenfalls einem gewissen Wandel unterworfen sind.

Da sich diese Rechtsprechung im Berichtszeitraum auch mehrmals mit dem Betrieb von Facebook Fanpages und dem Einsatz von Messengerdiensten befasste, ergaben sich auch hierzu laufend Fragen und Nachfragen von unterschiedlichen Seiten wie auch ein entsprechender Beratungsbedarf. Auch wenn insoweit immer noch keine einheitliche durchgängig klare Haltung zu erkennen ist, hat sich doch unterdessen, wenn auch vor allem nach Ablauf des Berichtszeitraums, jedenfalls im Kreise der Aufsichtsinstitutionen eine eher kritische Haltung jedenfalls wohl mehrheitlich durchgesetzt.

Ein immer wieder Nachfragen provozierendes Themenfeld bilden die Voraussetzungen, die gegeben sein müssen, um eine Meldepflicht für Datenschutzverletzungen auszulösen, wie auch die Frage, unter welchen Voraussetzungen welche Folgemaßnahmen erforderlich sind. Die mit dem Inkrafttreten der DS-GVO für Deutschland eingetretenen Veränderungen der Rechtslage haben hierzulande das Niveau, ab dem von einer meldepflichtigen Datenpanne auszugehen ist, sicherlich abgesenkt, was wohl einen maßgeblichen Teil des auftretenden Klärungsbedarfes bedingt haben dürfte.

Auf Seiten der Anbieter beschäftigte uns schließlich auch die Frage immer wieder, wie mit den gesetzlichen Löschpflichten umzugehen wäre, und welche Bedeutung dabei den bestehenden gesetzlichen Aufbewahrungs- und Archivierungsvorgaben zukommt und welche Tragweite davon ausgeht.

Wenngleich einen Anbieter steuerliche oder buchhalterische Aufbewahrungspflichten treffen können (vgl. dazu 3.2.2), so gilt das nicht automatisch für jegliche personenbezogene Daten in einem Kundenverhältnis, die er zu einem bestimmten Zeitpunkt oder für einen bestimmten vergangenen Zeitraum einmal rechtmäßig verarbeiten durfte. Hier ist nach Ansicht des Mediendatenbeauftragten aufgrund der Vorgaben aus Art. 30 Abs. 1 lit. F DS-GVO eine klare Kategorisierung von Datensätzen mit Festlegung von darauf bezogenen bestimmten Löschfristen erforderlich, die ein Verantwortlicher ggf. auch in sein Verarbeitungsverzeichnis aufzunehmen und deren Einhaltung er dann zu gewährleisten und nötigenfalls auch nachzuweisen hat.

### 3.5.2 Rundschreiben

Neben der individuellen Kommunikation mit Anbietern zu jeweils durch diese an uns herangetragene Fragestellungen werden zu bestimmten Themen in unregelmäßigen Abständen auch Informationsschreiben an alle Anbieter, ihre Geschäftsführer bzw. ihre Datenschutzbeauftragten erstellt und verschickt, die sich dann jeweils mit einem Themenbereich befassen, der nach unserer Auffassung von allgemeinem Interesse sein sollte.

Im Berichtszeitraum wurden ein solches Informationsschreiben im engen zeitlichen Zusammenhang mit der verbindlichen Geltung der DS-GVO ab dem 25.05.2018 verschickt. Neben dem Inkrafttreten der DS-GVO befasste sich dieses Rundschreiben vor allem mit den Auswirkungen, die davon auf die Fortgeltung des Telemediengesetzes und dabei insbesondere der Datenschutzregeln der §§ 11 ff TMG ausgehen würden, welche bis dahin aufgrund einer dynamischen Verweisung des RStV die maßgeblichen datenschutzrechtlichen Grundlagen für Rundfunkveranstalter bildeten. Diese Thematik betraf generell die Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste, also in aller Regel auch die Nutzung von Onlineverbindungen zur Rundfunkübertragung, sich daran anschließende Prozesse, z. B. im Rahmen von HbbTV, aber auch die Nutzung von Websites in vielerlei Beziehung, sodass die Bedeutung für den Rundfunksektor entsprechend groß war.

Das zweite Informationsschreiben aus dem November 2019 befasste sich mit der bereits dargestellten (vgl. oben 2.4) Orientierungshilfe für Teleme-

dienanbieter der DSK, die inhaltlich vorgestellt und in einem gewissen Rahmen erläutert wurde. In diesem Rahmen wurde auch die Planung vorgestellt, Informationsveranstaltungen für Anbieter zu diesem Themenkreis anzubieten. Diese Planung war in 2020 bereits weitgehend umgesetzt; die Durchführung fiel dann der Coronakrise zum Opfer, wird aber nachgeholt, sobald die äußeren Umstände dies zulassen.

## 3.6 Zahlen und Fakten im Überblick

Im Folgenden wird abschließend ein kurzer Überblick über den Umfang der bearbeiteten Fälle und dessen Entwicklung gegeben. Der vorliegende Bericht bezieht sich wegen des Geltungsbeginns der DS-GVO auf den Zeitraum vom 25.05.2018 bis 31.12.2019, also gut eineinhalb Jahre. Da die zu betrachtenden Zeiträume in den beiden Jahre 2018 und 2019 im Berichtszeitraum nur schwer vergleichbar sind, geht es hier eher darum aufzuzeigen, wie sich die Fallzahlen im Zeitraum insgesamt entwickelt haben, welche Entwicklungstendenzen es dabei gab und worauf diese zurückzuführen sein könnten.

Zu Beginn des Berichtszeitraums waren insgesamt 14 Fälle offen und wurden in die hier vorliegenden Zahlen aufgenommen. Im Zeitraum vom 25.05.2018 bis einschließlich 31.12.2018 wurden 76 neue Verfahren begonnen: So gab es in diesem Zeitraum 90 laufende Aufsichtsverfahren. Lediglich zwei davon waren gemeldete Datenpannen; die übrigen 88 Fälle waren Beschwerdeverfahren. Wir gehen davon aus, dass mit Geltung der DS-GVO und der entsprechenden Wahrnehmung in der breiten Öffentlichkeit auch eine gesellschaftliche Sensibilisierung stattgefunden hat, die dazu führte, dass man sich der in der DS-GVO beschriebenen Rechte bewusster wurde, deren Beachtung und die Einhaltung der Datenschutzvorgaben in einem verstärkten Maße erwartete und daher die zur Verfügung stehenden Rechte auch häufiger in Anspruch nahm. Im Berichtszeitraum konnten im Jahr 2018 41 Fälle abgeschlossen werden; 49 dieser Fälle wurden ins Jahr 2019 übertragen, wobei in den ersten Wochen des neuen Jahres 22 dieser Fälle abgeschlossen werden konnten.

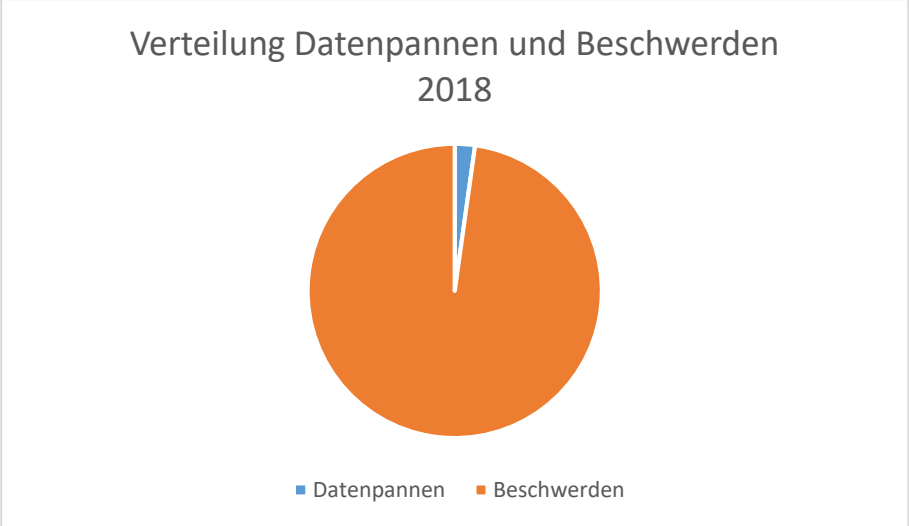
Im Jahr 2019 traten mit den soeben genannten insgesamt 165 Fälle auf. Interessant ist, dass nun ein deutlicher Anstieg der Datenpannen, nämlich 60 Fälle, im Vergleich zu den Beschwerden (105 Fälle) zu verzeichnen war.

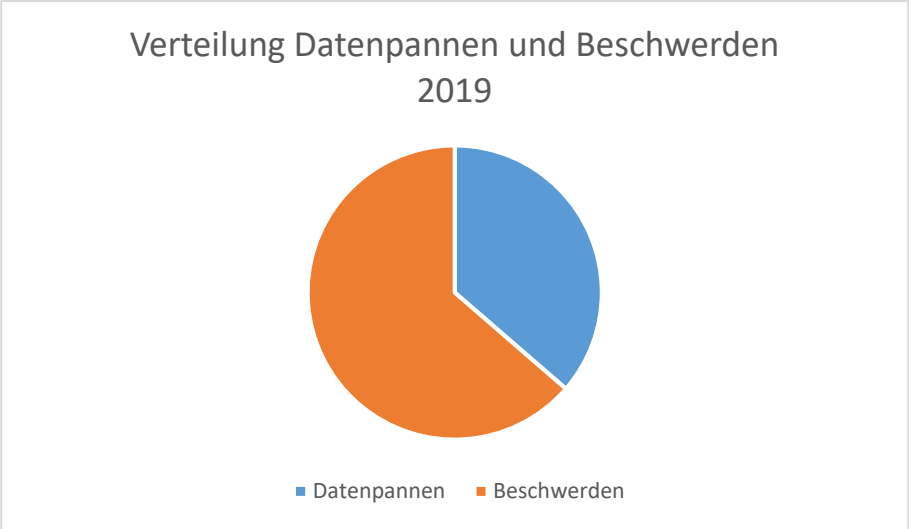
Ein Grund für diesen Anstieg der Datenpannen könnte die stärkere Sensibilisierung der Unternehmen und die Bedeutung sein, die Datenpannen im Laufe der Zeit beigemessen wurde. So könnte möglicherweise auch eine Rolle gespielt haben, dass Datenpannen aus anderen Bereichen, - die nicht unter unsere Zuständigkeit fielen - zu medialen Großereignissen wurden.

Vorrangig handelte es sich bei den uns gemeldeten Datenpannen um Fehlversendungen, aber auch die sonstige Offenlegung von Daten, Phishingfälle, verlorene Datenträger und die versehentliche Veröffentlichung von Kundendaten waren darunter.

Zum größten Teil waren die Meldungen der Pannen in zutreffender Weise erfolgt. In manchen Fällen war die Einhaltung der dabei zu beachtenden gesetzlichen Vorgaben und hierbei insbesondere derjenigen einer unverzüglichen Meldung bei Bekanntwerden der Datenschutzverletzung zweifelhaft. Der entsprechende Anbieter wurde jeweils auf die grundsätzlich bestehenden und zu beachtenden gesetzlichen Vorgaben einschließlich der einschlägigen Meldefrist hingewiesen. Eine Verzögerung sollte nur in komplexen Einzelfällen vorkommen und ist bei der Meldung entsprechend zu begründen.

Die untenstehenden Grafiken zeigen deutlich diese Entwicklung des Datenpannenanstiegs im Vergleich zu den Beschwerden.






Im Jahr 2019 wurden insgesamt 116 Verfahren abgeschlossen und 49 Fälle ins neue Jahr 2020 übertragen. Zu Beginn des Jahres 2020 konnte jedoch ein Großteil der übertragenen Fälle abgeschlossen werden. Und auch hier lässt sich festhalten, dass sich der Trend des Anstiegs der Datenpannen fortsetzt.

## 3.7 Ausblick

Im Berichtszeitraum lag ein Schwerpunkt der Tätigkeit des Medienbeauftragten für den Datenschutz in der fallspezifischen Beratung von Anbietern. Dies wird wohl auch im kommenden Berichtszeitraum der Fall sein. 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.

Um dies zu ermöglichen, plant der Medienbeauftragte Informationsveranstaltungen für Anbieter anzubieten, in denen diesen der Inhalt der DS-GVO nahegebracht und die dazugehörige Rechtsauffassung der Aufsicht dargelegt wird; zudem soll die Möglichkeit des Austausches unabhängig von konkreten Aufsichtsfällen geboten werden (vgl. 2.4).

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

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

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

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

Anlasslosen Prüfungen vorgelagert sind anbieterübergreifende Basisuntersuchungen z. B. zur datenschutzkonformen Ausgestaltung von Websites vorgesehen, die einen Überblick über die Marktgegebenheiten im Zuständigkeitsbereich vermitteln sollen. Aus diesen Untersuchungen können sich dann wiederum konkrete Bedarfe für Unterrichtungen und Informationsveranstaltungen, aber auch gegebenenfalls für die Einleitung von Aufsichtsverfahren ergeben. Gleichwohl wird die Grundausrichtung der Aufsichtstätigkeit unverändert zunächst darin liegen, die gesetzlichen Vorgaben bekanntzumachen und auf deren Einhaltung zu drängen.