Landtag von Baden-Württemberg **Drucksache 17 / 8646**

17. Wahlperiode **2.4.2025**

Mitteilung

des Rundfunkdatenschutzbeauftragten

Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten für den Zeitraum 1. Januar 2024 bis 31. Dezember 2024

Schreiben des Rundfunkdatenschutzbeauftragten vom 4. April 2025

Anbei übersende ich Ihnen meinen Tätigkeitsbericht für das Jahr 2024.

Den jährlichen Tätigkeitsbericht erstatte ich gemäß § 27 Absatz 10 Landesdatenschutzgesetz Baden-Württemberg den Organen des SWR sowie den Landtagen und den Landesregierungen der unterzeichnenden Länder des Staatsvertrags über den Südwestrundfunk.

Schwarze

Eingegangen: 2.4.2025 / Ausgegeben: 10.4.2025

Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: www.landtag-bw.de/Dokumente

Der Landtag druckt auf Recyclingpapier, ausgezeichnet mit dem Umweltzeichen „Der Blaue Engel“.

BR hr mdr rbb SR SWR WDR ZDF Deutschlandradio

TÄTIGKEITS BERICHT

des Rundfunkdatenschutzbeauftragten

24

Der Rundfunkdatenschutzbeauftragte

Stephan Schwarze

Kantstraße 71-73, 04275 Leipzig

www.rundfunkdatenschutz.de

Leipzig, März 2025

Berichtszeitraum: 01.01.2024 bis 31.12.2024

Inhaltsverzeichnis

Vorwort **7**

1 Einleitung **9**

2 Aufgaben und Befugnisse des Rundfunkdatenschutzbeauftragten **9**

2.1 Gesetzliche Grundlagen **9**

2.2 Zuständigkeit bei Rechtsverletzungen durch Berichterstattung **11**

3 Entwicklungen im Datenschutzrecht **12**

3.1 EU-Datenstrategie **12**

3.2 Artificial Intelligence Act (AIA) / KI-Verordnung (KI-VO) **13**

3.3 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) **14**

3.4 Entwurf Beschäftigtendatengesetz (BeschDG) **15**

3.5 Entwurf Reformstaatsvertrag **15**

3.6 Rechtsprechung **18**

3.6.1 Aktuelles zum Umfang des Auskunftsanspruchs 18
3.6.2 Beschäftigtendatenschutz - Kollektivvereinbarungen 19
3.6.3 Leitsatzentscheidung zu Scraping 20
3.6.4 Keine Verpflichtung zu Abhilfemaßnahmen durch Aufsichtsbehörden 21

3.7 EDSA-Stellungnahmen und Leitlinien **22**

3.7.1 Stellungnahme zu bestimmten Verpflichtungen, die sich aus der Abhängigkeit von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben 22
3.7.2 Leitlinien für die Rechtsgrundlage des berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f DSGVO 22
3.7.3 Stellungnahme zur Verwendung personenbezogener Daten für die Entwicklung und Einführung von KI-Modellen 23
3.7.4 Datenschutzleitfaden für kleine Unternehmen 24

4 Eingaben beim Rundfunkdatenschutzbeauftragten **25**

4.1 Beschwerden **26**

4.2 Sonstige Eingaben **27**

5 Meldungen nach Art. 33 DSGVO 28

6 Themen und Schwerpunkte der Aufsicht 30

6.1 Audit Nutzungsmessung 30

6.1.1 Fragenkatalog und Auswertung 31
6.1.2 Ergebnisse 32
6.1.3 Nachfragen 33
6.1.4 Auditbericht und Ausblick 34

6.2 Nutzungsmessung durch Piano Analytics 35

6.3 Einführung lineare Nutzungsmessung HbbTV 37

6.4 Künstliche Intelligenz 38

6.5 Befragung zu Onboarding und Schulung 39

6.6 Geplantes Audit von Nachrichten-Apps 40

6.7 Medienprivileg 41

6.7.1 Rechtsgrundlagen und Anwendbarkeit des Medienprivilegs 41
6.7.2 Kommentare auf Facebook-Kanal 43
6.7.3 Subsidiäre Aufsichtszuständigkeit 43
6.7.4 Correctiv - Wem gehört die Stadt ? 44

6.8 Erfüllung Informationspflichten gegenüber Beschäftigten 44

6.9 Datenauswertung freie Mitarbeitende 46

6.10 Führung des VVT durch interne Datenschutzbeauftragte 48

6.11 Altersfreigabe in der ARD- und ZDF-Mediathek 49

6.12 Rechnungshöfe und Datenschutz 50

6.13 Nutzung von WhatsApp im Rahmen der Zuschauerkommunikation 51

6.14 Gewinnspiel 52

7 Datenschutz in den Rundfunkanstalten 53

7.1 Quartalsweiser Austausch mit den Rundfunkanstalten 53

7.1.1 Organisation des Datenschutzes 54
7.1.2 Stellung und Aufgaben der internen Datenschutzbeauftragten 54
7.1.3 Berichtsweg an das Management 56
7.1.4 Einführung bzw. Weiterentwicklung eines Datenschutz-Managementsystems 56
7.1.5 Beschwerden und Auskunftsanfragen 57

7.1.6 Kontinuierliche Themenschwerpunkte in den Rundfunkanstalten 57
7.2 Überprüfung der Datenschutzhinweise auf Homepages der Rundfunkanstalten 58
8 Datenschutz beim Beitragsservice 59
8.1 Kostenpflichtiger Online-Service für Rundfunkbeitragsangelegenheiten 59
8.2 Beschwerdevorlagen gegen die Datenverarbeitung beim Beitragsservice und die Datenweitergabe an Vollstreckungsbehörden 60
8.3 Unterlassungsaufforderungen - Anfragen von Meldebehörden 61
8.4 Verarbeitung von Gesundheitsdaten 62
8.5 Löschung von Bankdaten 63
8.6 Datenweitergabe an Gerichtsvollzieher 65
8.7 Adresshandel 66
9 Rundfunkdatenschutzkonferenz (RDSK) 67
9.1 Aufgaben der RDSK 67
9.2 Handreichungen, Empfehlungen und Orientierungshilfen 69
9.2.1 Orientierungshilfe KI 69
9.2.2 Listen zur Datenschutzfolgenabschätzungen 72
9.2.3 Grundlagen für die Verhängung von Bußgeldern 72
10 Arbeitskreis der Datenschutzbeauftragten (AK DSB) 73
10.1 Organisatorische Weiterentwicklung 73
10.2 Austausch im AK DSB 73
11 Austausch mit der Datenschutzkonferenz (DSK) 74
11.1 AK Medien 76
11.2 AK Grundsatz 76
11.3 AK Technik 77
11.4 AK KI 77
12 Ausblick und Schlussbemerkung 78
13 Anhang 80
13.1 DSGVO Art. 51 ff. 80

13.2 DSGVO Art. 85 85
13.3 MStV § 12, § 23, § 113 86
13.4 TDDDG § 25 88
13.5 Regelungen zum Rundfunkdatenschutzbeauftragten 89
13.6 RDSK-Mitgliederliste 91
13.7 RDSK-Verwaltungsvereinbarung 92

Vorwort

Die Datenschutzaufsicht über insgesamt neun Landesrundfunkanstalten[1] ist vielfältig, in den Ausprägungen abwechslungsreich und in rechtlicher Hinsicht dynamisch, „ruhigeres Fahrwasser“ kann ich nicht vermelden. Dies ist auch nicht das Ziel, das Wesen der Aufsicht – so wie ich es verstehe – besteht darin, sich einzumischen und mitzuwirken. Regelmäßig führe ich Audits oder Datenschutzprüfungen bei den Rundfunkanstalten durch und lade zu Jour fixes. Daneben sind zahlreiche Beschwerden zu bearbeiten und Anfragen der Rundfunkanstalten zu beantworten. Rechtliche Neuerungen, wie die nunmehr in Kraft getretene KI-Verordnung, müssen in den Blick genommen und Ableitungen für die Aufsichtstätigkeit identifiziert werden. An spannenden Themen und Betätigungsfeldern mangelt es also nicht.

Ebenso hat der Versuch einer Verbesserung der Zusammenarbeit mit den staatlichen Aufsichtsbehörden, der Datenschutzkonferenz und den aus ihr hervorgegangenen Arbeitskreisen einen nicht unerheblichen Raum in meiner Tätigkeit eingenommen. Insbesondere bemühen sich die Rundfunkdatenschutzbeauftragten nach wie vor, als vollwertige Aufsichtsbehörden i.S.d. DSGVO behandelt und wahrgenommen zu werden – so wie es das Gesetz vorsieht. Ungeachtet der guten Zusammenarbeit auf Arbeitsebene gibt es noch vieles zu verbessern, und ich fühle mich aufgerufen, dies stets aufs Neue anzumahnen und entsprechende Vorschläge zu unterbreiten.

Bedeutsam war im Berichtsjahr 2024 der Beschluss der Regierungschefinnen und Regierungschefs der Länder vom Oktober 2024 zum Staatsvertrag zur Reform des öffentlich-rechtlichen Rundfunks. In diesem Regelwerk findet sich auch der gemeinsame Rundfunkdatenschutzbeauftragte wieder, der von den in der ARD zusammengeschlossenen Landesrundfunkanstalten, dem ZDF und dem Deutschlandradio ernannt werden muss. Eine aus meiner Sicht sehr wichtige Verankerung des gemeinsamen Rundfunkdatenschutzbeauftragten im Gesetz und damit eine wohl bald verwirklichte Institutionalisierung, die sowohl die Ausübung des Amtes befördert als auch die Wirksamkeit der Behörde stärkt (siehe dazu auch Kapitel 3.5).

Im Berichtsjahr konnte ich auf die Unterstützung einer Referentin, eines Referenten und einer Assistentin zurückgreifen. Damit war es mir möglich, wesentlich weitgefächerter meinen Aufgaben nachzugehen, was sich in den Datenschutzprüfungen und Audits niederschlug. Ebenso war auch Raum für die eingehende Beschäftigung mit dem Datenschutzrecht und daraus erwachsenen Pflichten für die Rundfunkanstalten. Daraus entstehen möglichst gemeinsam mit der RDSK Arbeitspapiere, die nach meiner Erfahrung als hilfreich wahrgenommen werden. Dies im Übrigen auch gern in Zusammenarbeit mit den staatlichen Aufsichtsbehörden, was sich allerdings, wie oben angedeutet, als nicht ganz einfach erweist.

[1] Deutschlandradio ist eine Körperschaft, der Einfachheit halber wird jedoch stets von Rundfunkanstalten gesprochen.

Ich danke insbesondere meinen Mitarbeiterinnen und meinem Mitarbeiter für die äußerst engagierte und auch auf der menschlichen Ebene sehr angenehme Zusammenarbeit. Dies gilt ebenso für die internen Datenschutzbeauftragten der von mir beaufsichtigten Rundfunkanstalten; die Arbeit im Rahmen des AK DSB und auch der sonstige Austausch hat sich als erfreulich und fruchtbar erwiesen. Mein herzlicher Dank gebührt allen Genannten.

Im Berichtsjahr 2024 ist meiner Behörde einiges gelungen, vieles befindet sich immer noch in der Aufbauphase und manches mag auch nicht in der vorgesehenen Weise geglückt sein. Ich bin aber zuversichtlich, dass wir es auch künftig schaffen werden, sowohl den Betroffenen als auch den Rundfunkanstalten gerecht zu werden und die Herausforderungen zu meistern.

Ich wünsche allen Leserinnen und Lesern eine möglichst kurzweilige Lektüre, ein Grundinteresse an datenschutzrechtlichen Themen kann dabei gewiss nicht schaden.

Leipzig, im März 2025
Stephan Schwarze

1 Einleitung

Nach Art. 59 DSGVO legt der Rundfunkdatenschutzbeauftragte als Aufsichtsbehörde einen Jahresbericht über seine Tätigkeit vor. Die für die gemeinsame Aufsicht über acht Rundfunkanstalten maßgeblichen Vorschriften sehen vor, dass ich diesen Bericht den Organen zur Verfügung zu stellen habe[2]. Dies sind die Verwaltungsräte, die Rundfunk-, Hörfunk- oder Fernsehräte sowie die Intendantinnen und Intendanten, die ich förmlich über meinen Bericht unterrichte. Meiner Veröffentlichungspflicht komme ich nach, in dem ich den Bericht auf meiner Website www.rundfunkdatenschutz.de zur Verfügung stelle. Die jeweiligen Landesregierungen und Parlamente, darunter die für das ZDF und das Deutschlandradio jeweils aktuell rechtsaufsichtsführenden Länder werden ebenfalls von der Veröffentlichung des Berichts in Kenntnis gesetzt.

2 Aufgaben und Befugnisse des Rundfunkdatenschutzbeauftragten

Seit dem Jahr 2023 nehme ich gemeinsam für BR, HR, MDR, rbb, SR, SWR, WDR, Deutschlandradio und ZDF sowie die von ihnen verantworteten Gemeinschaftseinrichtungen und ihre Beteiligungsunternehmen die datenschutzrechtliche Aufsicht wahr. In diesem Kapitel wird über die Besonderheiten der gemeinsamen Aufsicht sowie die gesetzlich zugewiesenen Aufgaben informiert.

2.1 Gesetzliche Grundlagen

Der nach den Landesvorschriften (Art. 21 Abs. 1 Bayerisches Rundfunkgesetz, § 28 Abs. 2 Hessisches Datenschutz- und Informationsfreiheitsgesetz, § 38 Abs. 1 MDR-Staatsvertrag, § 47 Abs. 1 rbb-Staatsvertrag, § 24 Abs. 1 SR-Gesetz, § 39 Abs. 1 SWR-Staatsvertrag i.V.m. § 27 Abs. 1 Landesdatenschutzgesetz Baden-Württemberg, § 49 Abs. 1 WDR-Gesetz, § 16 Abs. 1 Deutschlandradio-Staatsvertrag, § 16 Abs. 1 ZDF-Staatsvertrag) ernannte Rundfunkbeauftragte für den Datenschutz ist zuständige Aufsichtsbehörde im Sinne der DSGVO.

Beim Bayerischen Rundfunk, Mitteldeutschen Rundfunk, Hessischen Rundfunk, Rundfunk Berlin-Brandenburg, Westdeutschen Rundfunk, Deutschlandradio und ZDF erfolgt die Ernennung für die Dauer von vier Jahren, beim Saarländischen Rundfunk und beim Südwestrundfunk für die Dauer von sechs Jahren. Das Amt des Rundfunkdatenschutzbeauftragten ist unabhängig ausgestaltet, er unterliegt insbesondere keiner Rechts- oder Fachaufsicht. Beim BR, MDR, rbb, WDR,

[2] Eine solche Vorschrift fehlt beim Hessischen Rundfunk. Es wird gleichwohl so wie bei den anderen Rundfunkanstalten gehandhabt.

Deutschlandradio und ZDF ist geregelt, dass die vom Verwaltungsrat ausgeübte Dienstaufsicht diese Unabhängigkeit keinesfalls beeinträchtigen darf. Nach § 27 Abs. 5 Landesdatenschutzgesetz Baden-Württemberg unterliegt der Rundfunkdatenschutzbeauftragte beim SWR im Gegensatz dazu keiner Dienstaufsicht. Gemäß § 28 Abs. 2 Hessisches Datenschutz- und Informationsfreiheitsgesetz überwacht der Rundfunkdatenschutzbeauftragte den Datenschutz im journalistischen Bereich frei von Weisungen. Damit ist die Unabhängigkeit in vollständiger Weise umgesetzt.

In seiner Funktion als Aufsichtsbehörde ist der Rundfunkdatenschutzbeauftragte zuständig für die Einhaltung des Datenschutzes bei den Rundfunkanstalten in ihren gesamten Tätigkeiten, aber auch bei deren Beteiligungsunternehmen.[3] Die Aufgaben und Befugnisse ergeben sich insbesondere aus den Artikeln 57 und 58 DSGVO.

Jede oder jeder kann sich an den Rundfunkdatenschutzbeauftragten wenden, wenn sie oder er der Ansicht ist, bei der Verarbeitung ihrer oder seiner personenbezogenen Daten durch die Rundfunkanstalten oder eines ihrer Beteiligungsunternehmen in ihren oder seinen Rechten verletzt worden zu sein. Hinzu kommen die Aufgaben nach Artikel 57 DSGVO, wonach insbesondere die Datenschutzgrundverordnung zu überwachen und durchzusetzen ist. Dort ist auch geregelt, dass der Rundfunkdatenschutzbeauftragte an der Sensibilisierung der Verantwortlichen, der betroffenen Personen und der Öffentlichkeit mitzuwirken hat und mit anderen Aufsichtsbehörden zusammenarbeiten soll.

Ebenso besteht die Pflicht, Datenschutzverstöße gegenüber der Intendantin oder dem Intendanten der jeweiligen Rundfunkanstalt zu beanstanden und sie zu einer Stellungnahme aufzufordern. Eine gleichzeitige Unterrichtung des Verwaltungsrates oder des Rundfunkrates (beim Hessischen Rundfunk) ist vorgesehen; von einer förmlichen Rüge kann dann abgesehen werden, wenn es sich um einen vergleichsweise weniger gravierenden Mangel handelt oder wenn die unverzügliche Behebung des Verstoßes sichergestellt ist. In formaler Hinsicht mussten bei den Rundfunkanstalten im Berichtsjahr keine Beanstandungen ausgesprochen werden.

Artikel 58 DSGVO weist dem Rundfunkdatenschutzbeauftragten zudem hoheitliche Befugnisse zu, wonach die Verantwortlichen – also die Rundfunkanstalten bzw. ihre jeweiligen Beteiligungsunternehmen – auch per Verwaltungsakt zu Handlungen oder Unterlassungen verpflichtet werden dürfen, wenn dies nach Auffassung des Rundfunkdatenschutzbeauftragten erforderlich ist. Dazu gehört auch, dass Verarbeitungsvorgänge gänzlich untersagt werden können. Gegenüber den Rundfunkanstalten kann der Rundfunkdatenschutzbeauftragte keine Geldbußen

[3] Ausnahme Hessischer Rundfunk: Der Beauftragte für den Datenschutz überwacht den Datenschutz im journalistischen Bereich (§ 28 Abs. 2 S. 1 HDSIG).

verhängen (vgl. z.B. § 40 Abs. 1 S. 4 MDR-Staatsvertrag, § 27 Abs. 7 S. 2 LDSG BW, § 18 Abs. 1 S. 4 ZDF-Staatsvertrag), gegenüber Beteiligungsunternehmen ist dies jedoch möglich.[4]

2.2 Zuständigkeit bei Rechtsverletzungen durch Berichterstattung

Zahlreiche Eingaben und im Berichtsjahr auch eine Presseanfrage erreichten mich zu dem Thema, inwieweit der Rundfunkdatenschutzbeauftragte auch für Beschwerden bei Verletzungen von Persönlichkeitsrechten zuständig ist, die aufgrund von Berichterstattungen der Rundfunkanstalten vermutet werden.

Stets weise ich darauf hin, dass die §§ 12 und 23 Medienstaatsvertrag auf Basis von Art. 85 DSGVO die journalistische Datenverarbeitung weitgehend von den sonstigen datenschutzrechtlichen Vorgaben freistellen (ausführlich zum Medienprivileg siehe Kapitel 6.7 dieses Berichtes und ebenso Tätigkeitsbericht 2023, Kapitel 6.3). Hintergrund ist, dass journalistische Tätigkeit nicht mehr sinnvoll auszuüben und die für eine funktionsfähige demokratische Gesellschaft essenziellen Funktionen von Presse und Rundfunk ausgeschaltet wären, würden die allgemeinen Datenschutzregeln uneingeschränkt für diesen Bereich gelten. Folgerichtig ergibt sich aus der Systematik auch, dass in diesem Bereich die Datenschutzaufsicht nur untergeordnet bzw. in Teilaspekten, wie etwa der Datensicherheit und dem Datengeheimnis, zuständig ist. Ich weise auch stets darauf hin, dass die Rundfunkanstalten nicht völlig frei darin sind, ob und inwieweit sie z.B. in identifizierender Weise über Personen berichten. Auch die Rundfunkanstalten sind gehalten, dies nur im Rahmen der allgemeinen persönlichkeitsrechtlichen Grenzen zu tun, dies gehört zu ihrer journalistischen Sorgfaltspflicht.

Daraus folgt wiederum, dass die Prüfung einer solchen Persönlichkeitsrechtsverletzung nicht dem Rundfunkdatenschutzbeauftragten obliegt, denn eine solche (potenzielle) Verletzung ist jedenfalls keine des Datenschutzrechtes. Sollte jedoch eine Persönlichkeitsrechtverletzung durch die allgemeinen Gerichte oder auch durch die Rundfunkanstalten selbst festgestellt werden, kann die betroffene Person Auskunft über die der Berichterstattung zugrunde liegenden, zu ihrer Person gespeicherten Daten verlangen. Ebenso kann die betroffene Person unverzüglich Berichtigung unrichtiger personenbezogener Daten im diesbezüglichen Datensatz oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Diese Rechte ergeben sich aus § 12 Abs. 3 und § 23 Abs. 2 des Medienstaatsvertrages und sind wiederum vom Rundfunkdatenschutz-beauftragten zu prüfen.

Man erkennt an dieser Konstellation, dass diese Ausgestaltung auf den ersten Blick verwirrend sein kann, denn der Datenschutz lebt an dieser Stelle „nach“ einer Persönlichkeitsverletzung im

[4] Für die Bußgeldberechnung gelten die „Leitlinien 04/2022 für die Berechnung von Geldbußen im Sinne der DSGVO“ des Europäischen Datenschutzausschusses (EDSA).

Zusammenhang der dazu gespeicherten Daten wieder auf. Dies ist mir besonders im Rahmen einer Presseanfrage deutlich geworden, im Rahmen derer ich nur mit einiger Mühe Verständnis für diese Sach- und Rechtslage erzeugen konnte. Ebenso ist aber festzuhalten, dass eine Konstellation nach § 12 Abs. 3 oder § 23 Abs. 2 Medienstaatsvertrag in meiner bisherigen Praxis nicht vorgekommen ist.

3 Entwicklungen im Datenschutzrecht

Auch im Jahr 2024 gab es gesetzgeberische Entwicklungen, die das Datenschutzrecht unmittelbar betrafen oder mittelbar tangierten, vor allem auf EU-Ebene. Wesentlich im Jahr 2024 war das Voranschreiten der Regulierung von Künstlicher Intelligenz durch die KI-Verordnung, die auch im Lichte des Datenschutzrechts betrachtet werden muss. Daneben berichte ich von relevanter Rechtsprechung und gehe auf Stellungnahmen des Europäischen Datenschutzausschusses (EDSA) ein, die für die Auslegung des Datenschutzrechts prägend sind.

3.1 EU-Datenstrategie

Die EU-Datenstrategie, die bereits Eingang in den Tätigkeitsbericht 2023 gefunden hatte, wurde weiter vorangetrieben und manifestiert. So entfaltet der Digital-Services-Act (DSA), der ein sicheres vorhersehbares und vertrauenswürdiges Online-Umfeld und das Funktionieren des EU-Binnenmarktes gewährleisten soll, seit 17.02.2024 Wirkung. Mit besonderer Aufmerksamkeit wird zu beobachten sein, inwieweit der DSA der Tendenz einer Auflösung von selbstauferlegten Verhaltensregeln der Social-Media-Plattformen und der zunehmenden Duldung der Verbreitung von Desinformation im Internet, insbesondere durch Elon Musks Plattform „X“ sowie der dem folgenden Strategie des Meta-Konzerns von Mark Zuckerberg etwas entgegensetzen kann. Der deutsche Gesetzgeber hat mit dem Digitale-Dienste-Gesetz (DDG), das am 14.05.2024 in Kraft getreten ist, auf den DSA reagiert und die Plattformaufsicht neu geregelt, das Telemediengesetz (TMG) wurde in diesem Zusammenhang aufgehoben. Die Bundesnetzagentur soll danach die zuständige Koordinierungsstelle sein, die darüber wacht, dass Onlineplattformen und Suchmaschinen sich an den Rechtsrahmen des DSA halten und die auch gegen illegale Inhalte einschreiten soll. Der DSA und seine Durchsetzung fallen damit nicht in den Bereich der Datenschutzaufsicht. Gleichwohl gibt es Schnittmengen zwischen Plattformregulierung und Datenschutz, bei denen ein Austausch der Aufsichtsbehörden denkbar erscheint. Beispielsweise macht der DSA Vorgaben für Werbung auf Online-Plattformen und legt fest, dass bestimmte personenbezogene Daten nicht für kommerzielle Werbung verwendet werden dürfen. Im Übrigen

sei bezogen auf weitere Rechtsakte der EU-Datenstrategie (DMA, DGA, DA[5]) und die Relevanz für den Datenschutz im öffentlich-rechtlichen Rundfunk auf meine Ausführungen im Tätigkeitsbericht 2023 – Kapitel 3.1 - verwiesen.

3.2 Artificial Intelligence Act (AIA) / KI-Verordnung (KI-VO)

Zur KI-Verordnung habe ich im letzten Tätigkeitsbericht (Kapitel 3.1.5) bereits Stellung genommen. Künstliche Intelligenz hat sich im Jahr 2024 in rasanter Weise zu einem der wichtigsten gesellschaftlichen, technischen und rechtlichen Schwerpunktthemen entwickelt, das auch für die Aufsicht über den Datenschutz in den Rundfunkanstalten von hoher Priorität ist (siehe dazu auch Kapitel 6.4).

Am 01.08.2024 trat die KI-Verordnung/der Artificial Intelligence Act in Kraft, mit der die EU die verantwortungsvolle Entwicklung und Verwendung künstlicher Intelligenz fördern will. Einzelne Regelungsbereiche der KI-Verordnung entfalten nach Übergangsfristen nun schrittweise Geltung. Besondere Beachtung sollte dabei zunächst Art. 4 KI-VO erhalten.

„Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.“

Erhöhte Aufmerksamkeit ist deshalb erforderlich, da gemäß Art. 113 lit. a KI-VO die zitierte Regelung des Art. 4 KI-VO bereits seit 02.02.2025 gilt. Die sogenannte KI-Kompetenz muss ab diesem Datum durch die Anbieter und Betreiber von KI-Systemen nachgewiesen werden.

In Art. 3 Nr. 56 KI-VO wird definiert, was die KI-VO unter KI-Kompetenz versteht:

„KI-Kompetenz“ bezeichnet „die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden.“

KI-Kompetenz ist kurzgesagt also die Fähigkeit, KI sachkundig und risikobewusst einsetzen zu können. Auch wenn die KI-VO diese Kompetenz lediglich auf Basis der Verordnung selbst definiert, so ist gleichwohl der Datenschutz und die von der KI-VO ausdrücklich nicht angetastete DSGVO in

[5] Digital Markets Act (DMA), Data Governance Act (DGA), Data Act (DA)

sorgfältiger Weise zu berücksichtigen, wenn es darum geht, das Personal für die Risiken von KI zu sensibilisieren.

Es ist zu erwarten, dass dies auch die Rundfunkanstalten vor eine Herausforderung stellt. Die Verantwortlichen müssen durch geeignete Maßnahmen und Strukturen die KI-Kompetenz ihres Personals ertüchtigen. Das kann beispielsweise durch die Implementierung von internen Leitlinien und regelmäßigen Schulungen geschehen.

Die RDSK hat eine Orientierungshilfe entwickelt, die die wichtigsten Maßgaben bei der Anwendung von KI im öffentlich-rechtlichen Rundfunk aus Sicht des Datenschutzes, aber auch mit Rücksicht auf die KI-Verordnung beleuchtet und konkrete Handlungsempfehlungen sowie eine Checkliste beinhaltet (siehe Kapitel 9.2.1). Verknüpfungen dieser datenschutzrechtlichen Erwägungen mit den zu ergreifenden Maßnahmen zum Kompetenz-Aufbau aus der KI-VO sind wünschenswert.

Obwohl die Nichteinhaltung von Art. 4 KI-VO keine unmittelbaren Folgen für den Verantwortlichen nach sich zieht, so kann im Haftungsfall eine nachgewiesen unzureichende KI-Kompetenz als Sorgfaltspflichtverletzung angesehen werden und stellt insoweit ein nicht unerhebliches rechtliches Risiko dar.

3.3 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

National gab es eine gesetzgeberische Änderung, die nicht unerwähnt bleiben soll, auch wenn diese inhaltlich keine größeren Veränderungen nach sich zieht. Aus dem TTDSG (Telekommunikations-Telemedien-Datenschutz-Gesetz), das 2021 als nationale Umsetzung der ePrivacy-Richtlinie geschaffen wurde, wurde am 14.05.2024 das TDDDG (Telekommunikation-Digitale-Dienste-Datenschutzgesetz). Entscheidend für die Gesetzesumbenennung war die rein sprachliche Anpassung: aus „Telemediendienste“ wurden „Digitale Dienste“. Das TDDDG umfasst weiterhin spezifische Datenschutzvorschriften für Anbieter von Telekommunikationsdiensten (Telefonie, Internet) und digitalen Diensten (vor allem Websites, Apps), die die DSGVO ergänzen.

Am relevantesten bleibt dabei für die Rundfunkanstalten § 25 TDDDG (wie zuvor § 25 TTDSG). Danach ist die Speicherung von Informationen in der Endeinrichtung des Endnutzers (damit sind Geräte wie Smartphone oder Computer gemeint) oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind (Cookies und Local-Storage-Elemente) nur mit Einwilligung des jeweiligen Endnutzers zulässig. Ausnahmen bilden gemäß § 25 Abs. 2 Nr. 2 TDDDG Cookies und Local-Storage-Elemente, wenn die Datenverarbeitung unbedingt erforderlich ist, damit die Rundfunkanstalten „einen vom Nutzer ausdrücklich gewünschten Telemediendienst“ zur Verfügung stellen können. Um eine rechtskonforme Anwendung dieser Voraussetzungen sicherzustellen, hat

die RDSK 2022 Empfehlungen zum Einsatz von Cookies und Local-Storage-Elementen in Online-Angeboten der Rundfunkanstalten veröffentlicht und im August 2024 aktualisiert.

3.4 Entwurf Beschäftigtendatengesetz (BeschDG)

Eine weitere nationale Gesetzesinitiative betraf den bisher unterregulierten Beschäftigtendatenschutz. Der Beschäftigtendatenschutz soll in erster Linie den Schutz der Privatsphäre der Beschäftigten sicherstellen und muss in dieser Hinsicht mit dem Informationsinteresse des Arbeitgebers abgewogen werden.

Am 08.10.2024 wurde der Referentenentwurf des Bundesministeriums für Arbeit und Soziales und des Bundesministeriums des Innern und für Heimat eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt (Beschäftigtendatengesetz – BeschDG) bekannt. Der in Teilen europarechtswidrige § 26 Bundesdatenschutzgesetz (BDSG) sollte damit abgelöst werden. Auch aufgrund dieses unbefriedigenden Status quo fordern die Konferenz der unabhängigen Datenschutzbeauftragten (DSK) und die Bundesdatenschutzbeauftragte (BfDI) seit Jahren ein eigenständiges Beschäftigtendatenschutzgesetz.[6]

Durch das Scheitern der Ampelkoalition kam es jedoch nicht mehr zur Umsetzung des Gesetzesentwurfs. Da es aus heutiger Sicht unwahrscheinlich ist, dass eine andere Regierungskoalition das Gesetz in dieser Form aufgreift und beschließt, wäre es müßig, sich an dieser Stelle inhaltlich mit dem Entwurf auseinanderzusetzen. Für das datenschutzrechtlich anspruchsvolle Feld des Beschäftigtendatenschutzes ist die Nichtumsetzung jedenfalls ein Rückschlag, da schon längere Zeit Handlungsbedarf besteht. Es muss nun abgewartet werden, ob und in welcher Weise eine neue Bundesregierung einen neuen Anlauf unternimmt.

3.5 Entwurf Reformstaatsvertrag

Am 24. Oktober 2024 haben die Regierungschefinnen und Regierungschefs der Länder den Entwurf des Staatsvertrags zur Reform des öffentlich-rechtlichen Rundfunks beschlossen. In diesem auch Reformstaatsvertrag genannten Regelwerk finden sich einige Passagen zum Datenschutz. Im 4. Unterabschnitt „Datenschutz, Datenschutzaufsicht und Einsatz Künstlicher Intelligenz“ des

[6] Siehe: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20220429-Besch%C3%A4ftigtendatenschutz.html?nn=285748

Reformstaatsvertrages wird in § 31j die nach meiner Auffassung richtige neue Regelung zum gemeinsamen Datenschutzbeauftragten eingefügt. Dort heißt es in Abs. 1:

„Die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF und das Deutschlandradio ernennen einen gemeinsamen Rundfunkbeauftragten für den Datenschutz (Rundfunkdatenschutzbeauftragten), der zuständige Aufsichtsbehörde im Sinne des Artikels 51 der Verordnung (EU) 2016/679 ist".

Damit wird die institutionalisierte Verankerung des gemeinsamen Rundfunkdatenschutzbeauftragten als einheitliche Datenschutzaufsicht für den Rundfunk umgesetzt. Mein Vorgänger im Amt, Herr Dr. Reinhart Binder, hat im Vorwort seines Tätigkeitsberichts für das Jahr 2021 folgendermaßen formuliert: „Die Mandatierung eines gemeinsamen Rundfunkdatenschutzbeauftragten ist ein Musterbeispiel einer in jeder Hinsicht sinnvollen Kooperation im öffentlich-rechtlichen Rundfunk, die zugleich die rundfunkspezifische Datenschutzaufsicht gestärkt hat. Gleichwohl kann die bisherige Konstruktion das Effizienz- und Durchsetzungspotential einer echten Strukturreform (in Gestalt einer Aufsichtsbehörde für mehrere oder – besser noch – alle Rundfunkanstalten) nicht vollständig ausschöpfen."

Auch nach meinem Dafürhalten – und dies habe ich im Zuge meiner Stellungnahme zum Diskussionsentwurf zum Reformstaatsvertrag auch verdeutlicht – ist die gesetzliche Verankerung des gemeinsamen Rundfunkdatenschutzbeauftragten sinnvoll und wird von mir ausdrücklich begrüßt. Das Amt wird dadurch gestärkt und gewinnt Profil. Eine einheitliche Datenschutzaufsicht führt zu mehr Rechtssicherheit und Klarheit in der Anwendung der Vorschriften und trägt auch dazu bei, ein stabiles und einheitliches Datenschutzniveau in den Rundfunkanstalten, dem ZDF und Deutschlandradio zu gewährleisten und zu sichern.

Nachvollziehbar ist (wenngleich kompliziert in der Umsetzung), dass nach wie vor die Rundfunk-, Fernseh- und Hörfunkräte für die Ernennung des Rundfunkdatenschutzbeauftragten verantwortlich sind. Unter Berücksichtigung der vorgesehenen achtjährigen Amtszeit, die gleichsam die Unabhängigkeit der Aufsicht stärkt und sichert, ist dieses recht aufwendige Verfahren vernünftig.

Aktuell muss sich jedes Gremium nach den landesrechtlichen Vorschriften richten und auch die Amtszeiten des jeweiligen Rundfunkdatenschutzbeauftragten sind nicht überall gleich, ganz abgesehen davon, dass die Ernennung zu unterschiedlichen Zeitpunkten erfolgt ist. Dieses Thema „glatt zu ziehen", bringt erhebliche Vorteile auch für die Stellung und Wahrnehmbarkeit der Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk.

Ansonsten bleibt es bei den Pflichten der Aufsichtsbehörde, die sich – wie bei den staatlichen Aufsichtsbehörden auch – nach Kapitel VI. der DSGVO richten. Die Zuständigkeit, die Aufgaben sowie die Befugnisse sind dort ab Art. 51 DSGVO ausführlich beschrieben. Es gilt also: alle Aufsichtsbehörden haben im Rahmen der Geltung des europäischen Rechts die gleichen Aufgaben und Befugnisse.

Die Beschäftigung mit dem Entwurf des Reformstaatsvertrags war für mich auch aus einem anderen Blickwinkel hochinteressant. Die neuen und ausführlicheren Regelungen zum Auftrag des öffentlich-rechtlichen Rundfunks[7], insbesondere in § 26a des Reformstaatsvertrages, verpflichten zu regelmäßigen Angebotsüberprüfungen (Leistungsanalysen) und eröffnen die Möglichkeit, die zu diesem Zweck erforderlichen Daten rechtssicher zu verarbeiten. Leistungsanalysen haben nach diesen Regelungen auch unter dem Kriterium der quantitativen und qualitativen Nutzung der Angebote durch Zielgruppen zu erfolgen. Ebenso zu berücksichtigen sind Verfügbarkeit und Zugänglichkeit der Angebote und Inhalte sowie Wirkung der Angebote auf die individuelle Meinungsbildung der Nutzer und den öffentlichen Diskus. Der Gesetzgeber verpflichtet also den öffentlichen-rechtlichen Rundfunk, sehr genau nachzuhalten, wie der Auftrag erfüllt und ob den Anforderungen genügt wird. Aus den Erläuterungen zu diesen Vorschriften geht hervor, dass damit eine Betrachtung des Angebotes aus Nutzerperspektive erwartet und damit auch erlaubt wird. Dies eröffnet eine neue Perspektive auf die im Rahmen dieses Auftrags erforderliche Datenverarbeitung. Die vorgeschlagene Konkretisierung des Auftrages und die Verpflichtung, die Erfüllung dieses Auftrages auch zu dokumentieren, hat aus meiner Sicht – immer abhängig von den tatsächlich eingesetzten Mitteln – auch Auswirkungen auf die damit zusammenhängende und diesem Auftrag dienende Datenverarbeitung. Man wird also abwarten müssen, wie der öffentlich-rechtliche Rundfunk diese Verpflichtungen ausgestaltet und welche Hilfsmittel und Werkzeuge er einzusetzen gedenkt. Ich werde dies aus datenschutzrechtlicher Sicht sowohl kritisch als auch unterstützend begleiten und bin schon daher sehr gespannt auf die weiteren Entwicklungen.

Ob und in welcher Intensität eine Zunahme der datenschutzrechtlichen Befassung zu erwarten ist, bleibt zunächst dem im Jahr 2025 voraussichtlich zu verabschiedenden endgültigen Regelwerk und den sich aus den Vorschriften ergebenden Problemen vorbehalten.

Resümierend kann ich festhalten, dass die Etablierung eines gemeinsamen Rundfunkdatenschutzbeauftragten für den öffentlich-rechtlichen Rundfunk in institutioneller Hinsicht von großem Wert ist und die klarer ausgestalteten Auftragsanforderungen die Beurteilung der dafür erforderlichen Datenverarbeitung präzisieren und damit rechtssicherer gestaltbar machen dürften.

[7] Vgl. auch die aus datenschutzrechtlicher Sicht wichtigen §§ 26 Abs. 3, 30 Abs. 4, 36 Abs. 4 MStV-E

3.6 Rechtsprechung

Stets ist es auch erforderlich, die einschlägige Rechtsprechung zum Datenschutz, insbesondere auf europäischer Ebene, im Blick zu behalten. Mit diesem Kapitel soll über die wichtigsten Entscheidungen der Obergerichte informiert werden.

3.6.1 Aktuelles zum Umfang des Auskunftsanspruchs

Wie bereits im letzten Tätigkeitsbericht angesprochen (dort Kapitel 3.4.4), bleiben Auskunftsbegehren ein Themenfeld, das mich als Aufsicht jedes Jahr aufs Neue beschäftigt, so auch die Gerichte. Leitlinie für die Auslegung des Auskunftsrechts gemäß Art. 15 DSGVO im Allgemeinen sowie im Besonderen des Rechts auf Datenkopie aus Art. 15 Abs. 3 DSGVO bleibt das Urteil des EuGH vom 04.05.2023 (C-487/21). Anders als oft von Betroffenen verstanden, weitet das Recht auf Datenkopie das Auskunftsrecht des Art. 15 DSGVO nicht in seinem Anwendungsbereich oder in seinem Anspruchsinhalt aus. Es ist nicht zu verwechseln mit einem Recht auf Dokumenten- oder Akten-Kopie. Vielmehr, wie der EuGH bekräftigt, ist mit dem Begriff „Kopie“ gemeint, dass Betroffene eine originalgetreue und verständliche Reproduktion aller personenbezogenen Daten zur Verfügung gestellt bekommen. Anknüpfungspunkt bleiben die personenbezogenen Daten. Der europäische Datenschutzausschuss (EDSA) stellt in seinen Leitlinien ebenfalls klar, dass es sich bei der Kopie nicht um ein zusätzliches Recht der betroffenen Person handelt, sondern um eine „Modalität der Auskunftserteilung“[8].

Das Recht auf Kopie kann damit nicht über den Anwendungsbereich des Auskunftsrechts aus Art. 15 Abs. 1 DSGVO hinausreichen. Stattdessen ist vom Verantwortlichen zu prüfen, welche Dokumente und Verarbeitungsvorgänge personenbezogene Daten betreffen, und er hat dabei gemäß Art. 15 Abs. 4 DSGVO die Rechte und Freiheiten von anderen Personen zu berücksichtigen. Eine Herausgabe ganzer Dokumente oder auch von Auszügen aus Datenbanken, die personenbezogene Daten enthalten, die Gegenstand der Verarbeitung sind, ist damit nur im Ausnahmefall möglich. Laut EuGH ist die Zurverfügungstellung ganzer Dokumente lediglich dann unerlässlich, „wenn die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten“[9]. Diese Unerlässlichkeit der Herausgabe ist im Einzelfall genau zu prüfen. Der Bundesfinanzhof (BFH) hat sich im Urteil vom 12.03.2024 (IX R 35/21 - Rn. 28) mit der Frage der Unerlässlichkeit befasst und festgehalten, dass keine generelle Vermutung für die Unerlässlichkeit besteht, sondern dass es der betroffenen Person obliegt, „darzulegen, dass die Kopie der personenbezogenen Daten sowie die Mitteilung der Informationen nach Art. 15 Abs. 1

[8] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht | European Data Protection Board, Rn. 3, 16, 21 ff.
[9] EuGH, Urteil vom 04.05.2023 - C-487/21, NJW 2023, 2253 Rn. 41, 45

Buchst. a bis h DSGVO für die Wahrnehmung der ihr durch die Datenschutz-Grundverordnung verliehenen Rechte nicht genügt“.

Der BFH befasste sich in einem weiteren Urteil vom 12.11.2024 (IX R 20/22) mit der Zulässigkeit von auf Auskunft gerichteten Klageverfahren und nahm dabei auch eine Abgrenzung zum Akteneinsichtsrecht vor (vgl. auch bereits: BFH, Urteil vom 20.09.2024 - IX R 24/23). Art. 15 DSGVO beinhalte nach der Urteilsbegründung keinen Anspruch auf Akteneinsicht als "Weniger" zum Anspruch auf Zurverfügungstellung einer Kopie der personenbezogenen Daten, beziehungsweise ausnahmsweise unter bestimmten Umständen auf Zurverfügungstellung der Quellen, in denen die personenbezogenen Daten verarbeitet wurden. Vielmehr handele es sich bei der Gewährung von Akteneinsicht um ein Aliud, das auf dem Grundsatz des rechtlichen Gehörs (Art. 103 Abs. 1 des Grundgesetzes) beruhe. Das Recht auf Akteneinsicht eröffne die temporäre Möglichkeit zur Einsicht in die gesamte Verwaltungsakte, wohingegen das Auskunftsrecht aus Art. 15 DSGVO nicht auf die gesamte Akte abziele, sondern die dauerhafte Überlassung der darin enthaltenen personenbezogenen Daten herbeiführen wolle. Nur ausnahmsweise unter bestimmten Umständen sei die Auskunft gemäß Art. 15 DSGVO auf die Überlassung von Auszügen von Akten gerichtet.

Der BFH stellte in seinem Urteil vom 12.11.2024 zudem klar, dass eine Klage auf Auskunftserteilung gemäß Art. 15 DSGVO dann unzulässig ist, wenn es an einem dem Klageverfahren vorausgehenden außergerichtlich gestellten Antrag auf Auskunftserteilung fehlt. Das Gericht stellte dabei auf Art. 79 DSGVO ab, der für die Wahrnehmung von gerichtlichen Rechtsbehelfen voraussetzt, dass die Behörde zunächst Gelegenheit hatte, über den Auskunftsantrag zu entscheiden. Dies erscheint nachvollziehbar, denn wenn kein Antrag auf Auskunft (gilt auch bei anderen Betroffenenrechten) gestellt wird, das Recht also gar nicht ausgeübt wird, kann auch keine Verletzung eines Betroffenenrechts eintreten.

3.6.2 Beschäftigtendatenschutz - Kollektivvereinbarungen

Im Urteil vom 19.12.2024 (C-65/23) hat der EuGH sich mit der Datenverarbeitung im Beschäftigungskontext aufgrund von Kollektivvereinbarungen befasst. Kollektivvereinbarungen spielen teilweise auch in den Rundfunkanstalten eine Rolle als datenschutzrechtliche Rechtsgrundlage[10].

In der Entscheidung ging es um die Auslegung von Art. 88 DSGVO. Der EuGH stellte klar, dass auch bei der Anwendung von Kollektivvereinbarungen als Rechtsgrundlage zur Verarbeitung von Beschäftigtendaten die grundlegenden Anforderungen der DSGVO aus Art. 5, Art. 6 Abs. 1 sowie

[10] Beispielsweise im MDR die Rahmendienstvereinbarung über die Einführung und Anwendung informationstechnischer Systeme.

Art. 9 Abs. 1 und 2 DSGVO zu beachten sind. Datenschutzgrundsätze und Voraussetzungen, die an die Rechtsgrundlage gestellt werden, werden durch den Einsatz von Kollektivvereinbarungen also nicht ersetzt oder ausgehebelt, sondern bleiben trotz des Spielraums, der Art. 88 DSGVO den Parteien einräumt, weiter zu beachten. Eine gerichtliche Kontrolle der Vereinbarung müsse demnach speziell auf die Prüfung gerichtet sein, ob die Verarbeitung solcher Daten im Sinne der Art. 5, 6 und 9 DSGVO „erforderlich“ ist.

In der Konsequenz bedeutet dies, dass nationale Regelungen und Kollektiv- oder Betriebsvereinbarungen, die auf der Öffnungsklausel des Art. 88 DSGVO basieren, nicht unabhängig von den allgemeinen Grundsätzen der DSGVO betrachtet werden können. Diese klare Wertung des EuGH muss somit auch bei einer neuen Initiative zu einem Beschäftigtendatenschutzgesetz (dazu siehe auch Kapitel 3.4) Beachtung finden. Bestehende Kollektivvereinbarungen sollten durch die Verantwortlichen hinsichtlich der Anforderungen des EuGH überprüft werden.

3.6.3 Leitsatzentscheidung zu Scraping

Der Bundesgerichtshof (BGH) hat durch die erstmalige Nutzung des erst seit 01.11.2024 in der Zivilprozessordnung (§ 552b ZPO) eingeführten Entscheidungsart eines Leitentscheidungsverfahrens mit dem Urteil vom 18.11.2024 (VI ZR 10/24) Aufsehen erregt und schafft damit gleichzeitig eine klare Orientierung für die deutschen Gerichte, die die eher ungenauen EuGH-Entscheidungen[11] in diesem Themenkomplex bisher uneinheitlich auslegten. Diese neue Verfahrensart soll schnell höchstrichterliche Entscheidungen herbeiführen, wenn es eine Vielzahl von Verfahren mit vergleichbaren Rechtsfragen gibt und auch dann ergehen können, wenn die Revision zum BGH zwischenzeitlich zurückgezogen oder sich zuvor geeinigt wird.

Inhaltlich ging es um die häufig zu beobachtenden Schadensersatzprozesse, bei denen gemäß Art. 82 DSGVO ein immaterieller Schaden („Schmerzensgeld“) gefordert wird. Der BGH hat die Linie der Rechtsprechung damit deutlich verschoben. Bisher wurden Schadensersatzforderungen regelmäßig abgelehnt bei Fällen, in denen bloße Befürchtungen oder Ärgernisse über Datenschutzverletzungen vorgetragen wurden, bei denen es jedoch am Beweis konkreter negativer Folgen (das konnten auch Ängste oder Sorgen sein) des Betroffenen fehlte.

Der BGH urteilte nun aber, dass Betroffene keine besondere Beeinträchtigung nachweisen müssen und allein die Tatsache eines Kontrollverlusts der gegenständlichen personenbezogenen Daten für

[11] Z.B. EuGH Urteil v. 04.05.2023 – C-300/21; EuGH v. 11.12.2023 - C-340/21

die Annahme eines immateriellen Schadens ausreichen soll. Lediglich der Eintritt des konkreten Kontrollverlust muss nachgewiesen werden.

Vor allem für die oft ähnlich gelagerten Scraping-Fälle, bei denen im großen Stil von Unbekannten illegal Daten von Plattform-Nutzern (im Fall des BGH waren es Facebook-Nutzerdaten) abgegriffen und veröffentlicht oder zum Verkauf angeboten werden, hat diese Entscheidung eine enorme Tragweite. Ein höheres Prozessaufkommen ist damit zu erwarten. Allerdings macht der BGH auch klar, dass die Schmerzensgeldhöhe in der Regel als verhältnismäßig gering einzustufen sein wird. Der BGH spricht von Beträgen um 100 Euro. Ob die Betroffenen für diese eher geringen Beträge im Zweifel mehr Schadensersatzklagen führen, muss abgewartet werden; die Erfolgsaussichten derartiger Verfahren sind damit aber deutlich gestiegen. Das Wegfallen der Nachweispflicht eines konkreten Schadens stärkt jedenfalls die Rechte von Betroffenen.

Dass aber umgekehrt ein Kontrollverlust nicht pauschal angenommen werden kann, zeigt das Urteil des OLG Dresden vom 21.11.2024 (4 U 771/24). Ein Kontrollverlust kann dann nämlich nicht vorliegen, wenn der Nutzer eines sozialen Netzwerkes die von einem Scraping-Vorfall betroffenen Daten bereits vor diesem Ereignis auf einer eigenen Homepage zum Abruf bereitgehalten hat.

Auch in einem zweiten Verfahren vor dem OLG Dresden mit Urteil vom 10.12.2024 (4 U 815/24) wurde ein Kontrollverlust an Daten, die infolge eines Datenschutzverstoßes von einem sozialen Netzwerk "gescraped" wurden, abgelehnt, da die betreffenden Daten mit der Registrierung anzugeben und zwingend öffentlich für jedermann einsehbar waren.

3.6.4 Keine Verpflichtung zu Abhilfemaßnahmen durch Aufsichtsbehörden

Der EuGH befasste sich in seinem Urteil vom 26.09.2024 (C-768/21) mit der Frage, wie Datenschutzaufsichtsbehörden im Falle der Feststellung einer Verletzung des Schutzes personenbezogener Daten vorgehen müssen, bzw. in welchen Umfang Betroffene einen Anspruch auf Maßnahmen der Aufsichtsbehörde gegen die verantwortlichen Stellen haben. Dabei machte der EuGH klar, dass Aufsichtsbehörden nicht zwingend verpflichtet sind, Abhilfemaßnahmen zu ergreifen, wenn diese sich nicht als geeignet, erforderlich oder verhältnismäßig erweisen, um die festgestellten datenschutzrechtlichen Unzulänglichkeiten zu beseitigen. Beispielhaft nennt der EuGH Fälle, in denen der Verantwortliche umgehend die erforderlichen Maßnahmen ergreift und die Verletzung nicht wiederholt wird.

Das Urteil ist aus der Aufsichtsperspektive sehr zu begrüßen, da es die notwendige Flexibilität erhält, aufsichtsrechtliche Maßnahmen einzelfallbezogen und anhand der konkreten Umstände auszurichten. Für die Aufsichtsbehörde wird damit begrenzt durch das hohe Datenschutzniveau der

DSGVO ein Entscheidungsermessen zugesichert, in welcher Art und Weise sie der festgestellten Verletzung jeweils begegnet. Damit stärkt der EuGH auch die Unabhängigkeit der Aufsichtsbehörden.

3.7 EDSA-Stellungnahmen und Leitlinien

Das European Data Protection Board (edpb), das in Deutschland als Europäischer Datenschutzausschuss (EDSA) bezeichnet wird, soll eine einheitliche Anwendung der Datenschutz-Grundverordnung sicherstellen. Der EDSA veröffentlicht Stellungnahmen und Leitlinien zur Auslegung der DSGVO, die bei der Anwendung der DSGVO seitens der staatlichen Aufsichtsbehörden in Deutschland sowie auch im Hinblick auf meine Aufsichtstätigkeit Berücksichtigung finden.

Es würde den Rahmen dieses Berichts sprengen, detailliert über einzelne Stellungnahmen des EDSA zu berichten. Nachfolgend eine Auswahl dazu.

3.7.1 Stellungnahme zu bestimmten Verpflichtungen, die sich aus der Abhängigkeit von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben

Wenn Verantwortliche weisungsgebundene Auftragsverarbeiter für bestimmte Datenverarbeitungen einsetzen, werden Auftragsverarbeitungsverträge geschlossen und damit eine Reihe von gegenseitigen Pflichten vereinbart. Die Stellungnahme des EDSA vom 09.10.2024[12] befasst sich mit diesem anspruchsvollen Themenfeld und insbesondere mit acht Fragen zur Auslegung bestimmter Pflichten von Verantwortlichen, die sich auf Auftragsverarbeiter und Unterauftragsverarbeiter stützen. Dabei geht es auch um einzelne Formulierungen in Auftragsverarbeitungsverträgen, die sich aus Art. 28 DSGVO ergeben. Die Stellungnahme ist daher sehr praxisrelevant.

3.7.2 Leitlinien für die Rechtsgrundlage des berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f DSGVO

Ebenfalls am 09.01.2024 gab der EDSA Leitlinien für die Verarbeitung personenbezogener Daten auf Rechtsgrundlage des berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f DSGVO[13] heraus und

[12] https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_de
[13] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_de

formuliert darin Kriterien für die vorzunehmende Interessensabwägung bei der Verarbeitung personenbezogener Daten.

Zuerst muss danach ein berechtigtes Interesse des Verantwortlichen oder eines Dritten vorliegen, das als legitim angesehen werden kann. Ein solches muss rechtmäßig, klar und präzise formuliert und zudem real und gegenwärtig sein. In einem weiteren Schritt muss die Verarbeitung der jeweiligen personenbezogenen Daten auch zum Zwecke des berechtigten Interesses erfolgen und dafür erforderlich sein. Das heißt, das gewünschte Ziel darf nur mit Hilfe der konkreten Datenverarbeitung erreichbar sein. Wenn dagegen in gleicher Weise wirksame, aber aus Sicht des Datenschutzes weniger einschneidende Möglichkeiten zur Erreichung der verfolgten Interessen zur Verfügung stehen (Stichwort: Datenminimierung), fehlt es an dieser Voraussetzung. Im letzten Schritt erfolgt eine Interessenabwägung zwischen den Interessen, Rechten und Grundfreiheiten der betroffenen Person(en), die nicht gegenüber den legitimen Interessen des Verantwortlichen oder Dritten überwiegen dürfen.

Die Leitlinien geben neben der Definition der Voraussetzungen auch Beispiele für berechtigte Interessen und Hinweise, wie Abwägungen vorgenommen werden können. Bei Heranziehung der genannten Rechtsgrundlage für Datenverarbeitungen der Rundfunkanstalten und Beteiligungsunternehmen, können diese Hilfestellungen daher sensibilisierend sein. Auch für die Kontrolle und Bewertung durch die Aufsicht können die Leitlinien eine wertvolle Unterstützung darstellen.

3.7.3 Stellungnahme zur Verwendung personenbezogener Daten für die Entwicklung und Einführung von KI-Modellen

Große Bedeutung hat auch die EDSA-Stellungnahme zu KI-Modellen vom 18.12.2024[14], die eine europaweite Harmonisierung der momentan galoppierenden Entwicklung im Bereich der KI und auch der KI-Regulierung unterstützen soll.

In der Stellungnahme wird untersucht, ob KI-Modelle, die mit personenbezogenen Daten trainiert wurden, ebenfalls als personenbezogen einzuordnen sind oder ob sie stets als anonym betrachtet werden können. Im Ergebnis bleibt der EDSA aber vage in der Einschätzung. Er geht davon aus, dass in der Regel zwar keine personenbezogenen Daten in den KI-Modellen gespeichert sind, im Einzelfall aber enthalten sein können, mit der Folge, dass diese dann bei der Nutzung des KI-Modells wieder abgeleitet werden könnten. Die Erforderlichkeit einer präzisen Prüfung im Einzelfall kann folglich

[14] https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de

nicht entfallen, erst recht, da der für die Datenverarbeitung Verantwortliche in der Kontroll- und Dokumentationspflicht ist.

Der EDSA untersuchte auch, ob und wie das berechtigte Interesse gemäß Art. 6 Abs. 1 lit. f DSGVO als Rechtsgrundlage für die Entwicklung oder Nutzung von KI-Modellen verwendet werden kann. Er stellte fest, dass Art. 6 Abs. 1 lit. f DSGVO eine taugliche Rechtsgrundlage sein kann und es auf die Erforderlichkeit und die Interessenabwägung im Einzelfall ankomme.

Als dritten grundlegenden Untersuchungsgegenstand griff der EDSA die Frage auf, welche rechtlichen Folgen es für die Nutzung hat, wenn ein KI-Modell durch Verwendung unrechtmäßig verarbeiteter personenbezogener Daten entwickelt und trainiert wurde. Verstoßen werde nach Einschätzung des EDSA durch den Anbieter aufgrund eines datenschutzwidrigen Trainings von KI insbesondere gegen die Informationspflichten aus Art. 13, 14 DSGVO, die Löschpflichten aus Art. 17 DSGVO sowie gegen die Notwendigkeit von datenschutzfreundlicher Technikgestaltung nach Art. 25 DSGVO. Der EDSA beschreibt unterschiedliche Szenarien, die zu einer Rechtswidrigkeit der Nutzung des datenschutzwidrig trainierten Modells führen. Entscheidend sei dabei wiederum, ob im Rahmen der Anwendung des KI-Modells ein Personenbezug hergestellt werden könne. Wenn dies nicht der Fall ist, ist die Nutzung des datenschutzwidrig trainierten KI-Modells nach Einschätzung des EDSA aus datenschutzrechtlicher Sicht zulässig.

Mit dieser Stellungnahme wurden lediglich erste Pflöcke für die Bewertung von KI-Modellen eingeschlagen und erste Tendenzen erkennbar, wie der EDSA mit KI-Modellen umgeht. Es ist zu erwarten, dass noch weitere Stellungnahmen zur datenschutzrechtlichen Einschätzung zum Einsatz von KI folgen werden.

3.7.4 Datenschutzleitfaden für kleine Unternehmen

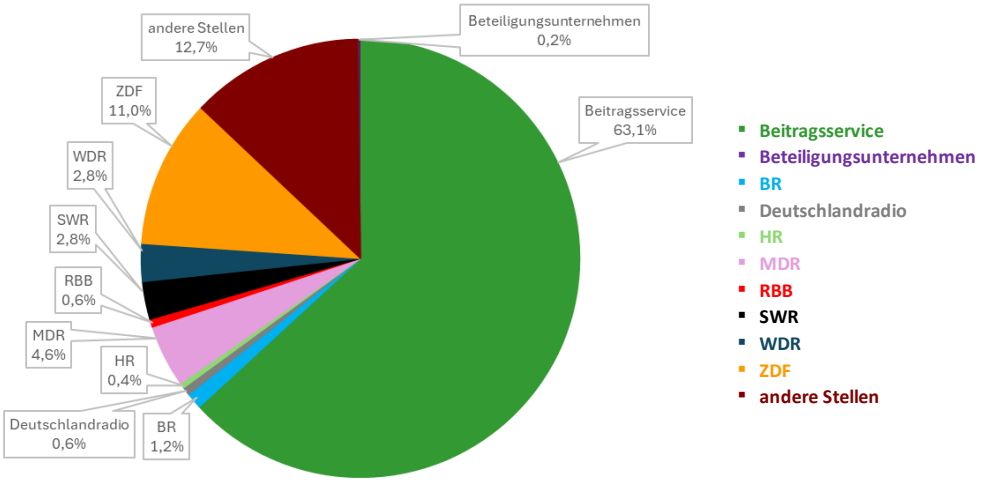
Im April 2024 veröffentlichte der EDSA den „Data-Protection-Guide for small business“ in einer deutschen Version[15]. Da dieser Leitfaden für kleinere Beteiligungsunternehmen eine anschauliche Hilfe sein kann, um die Datenschutzgrundlagen zu verstehen, und um einen sicheren und datenschutzkonformen Umgang mit personenbezogenen Daten und insbesondere auch mit Betroffenenrechten zu erreichen, weise ich an dieser Stelle darauf hin.

[15] https://www.edpb.europa.eu/sme-data-protection-guide/home_de

4 Eingaben beim Rundfunkdatenschutzbeauftragten

Der Rundfunkdatenschutzbeauftragte ist zuständig für die Bearbeitung von Beschwerden. Nach Art. 21 Abs. 6 BayRG i.V.m. Art. 57 Abs. 1 lit. f DSGVO, § 28 Abs. 2 Satz 2 Hessisches Datenschutz- und Informationsfreiheitsgesetz, § 40 Abs. 5 MDR-Staatsvertrag, § 47 Abs. 7 rbb-Staatsvertrag, § 27 Abs. 6 Landesdatenschutzgesetz Baden-Württemberg, § 51 Abs. 1 WDR-Gesetz i.V.m. Art. 57 Abs. 1 lit. f DSGVO, § 18 Abs. 5 Deutschlandradio-Staatsvertrag und § 18 Abs. 5 ZDF-Staatsvertrag kann sich jeder unmittelbar an ihn wenden, um eine Verletzung seiner Rechte vorzutragen. Im Übrigen wird das Recht auf Beschwerde bei einer Aufsichtsbehörde auch durch Art. 77 DSGVO gewährleistet.

Im Jahr 2024 erreichten die Aufsichtsbehörde 502 Eingaben:



Eingaben gesamt	Anzahl	Prozent
Beitragsservice	**317**	63,1%
Beteiligungsunternehmen	**1**	0,2%
BR	**6**	1,2%
Deutschlandradio	**3**	0,6%
HR	**2**	0,4%
MDR	**23**	4,6%
RBB	**3**	0,6%
SR	**0**	0,0%
SWR	**14**	2,8%
WDR	**14**	2,8%
ZDF	**55**	11,0%
andere Stellen	**64**	12,7%
Gesamt	**502**	100%

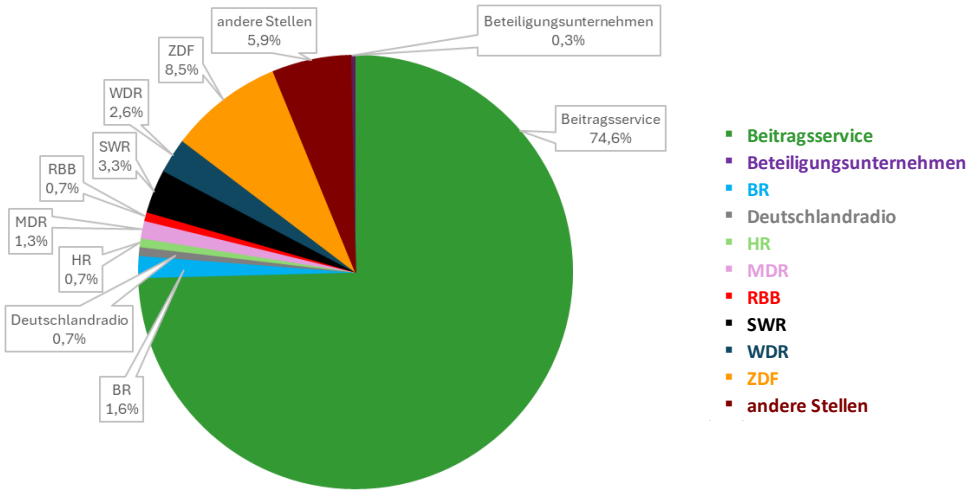
438 der Eingaben (87,3 %) konnten direkt den von meiner Behörde beaufsichtigten Rundfunkanstalten oder Beteiligungsunternehmen zugeordnet werden, 64 Eingaben (12,7 %) betrafen andere Einrichtungen/Stellen. Diese werden nachfolgend näher beschrieben.

Die Gesamtzahl der Eingaben unterteilte sich thematisch in:

- 307 Beschwerden (61,2 %) und
- 195 sonstige Eingaben (38,8 %).

4.1 Beschwerden

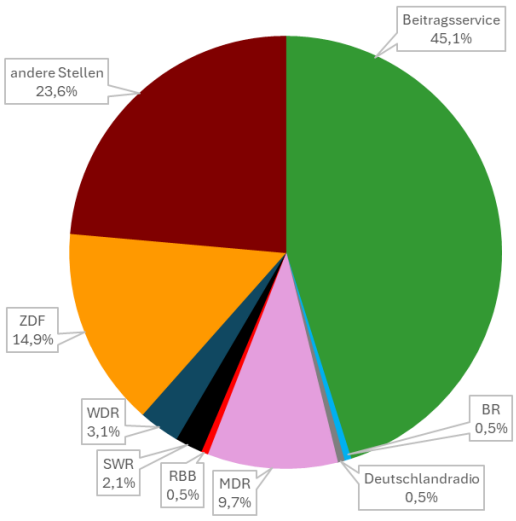
Die 307 eingegangenen Beschwerden verteilten sich wie folgt. Unter dem Punkt „andere Stellen“ sind Beschwerden zusammengefasst, die keiner spezifischen Rundfunkanstalt bzw. keinem spezifischem Beteiligungsunternehmen, die der Aufsicht unterliegen, zugeordnet werden konnten, so z.B. Beschwerden zu ARD, ARTE oder Privatsendern. Insgesamt 11 Beschwerden waren begründet (3,6 %).



Beschwerden	gesamt	Prozent	begründet	Prozent
Beitragsservice	**229**	74,6%	8	3%
Beteiligungsunternehmen	**1**	0,3%	1	100%
BR	**5**	1,6%	0	0%
Deutschlandradio	**2**	0,7%	0	0%
HR	**2**	0,7%	0	0%
MDR	**4**	1,3%	0	0%
RBB	**2**	0,7%	0	0%
SR	**0**	0,0%	0	0%
SWR	**10**	3,3%	0	0%
WDR	**8**	2,6%	2	25%
ZDF	**26**	8,5%	0	0%
andere Stellen	**18**	5,9%	0	0%
Gesamt	**307**	100%	11	
davon begründet	**11**	3,6%		

4.2 Sonstige Eingaben

Unter die sonstigen Eingaben werden Zuschriften gefasst, die von vermeintlichen Datenschutzthemen und fehlgeleiteten Auskunftsersuchen über Anfragen/Mitteilungen zum Beitragseinzug bis hin zur Beratung zu Datenschutzthemen reichen. Unter den 195 sonstigen Eingaben befanden sich 149 mit direktem Bezug zu einer Rundfunkanstalt (76,4 %). Unter dem Punkt „andere Stellen“ sind 46 Eingaben (23,6 %) zusammengefasst, die nicht direkt einer Rundfunkanstalt oder einem Beteiligungsunternehmen, die der Aufsicht unterliegen, zugeordnet werden konnten. Dabei handelt es sich z.B. um Eingaben bezüglich ARD oder Gemeinschaftseinrichtungen.



Sonstige Eingaben	Anzahl	Prozent
Beitragsservice	88	45,1%
Beteiligungsunternehmen	0	0,0%
BR	1	0,5%
Deutschlandradio	1	0,5%
HR	0	0,0%
MDR	19	9,7%
RBB	1	0,5%
SR	0	0,0%
SWR	4	2,1%
WDR	6	3,1%
ZDF	29	14,9%
andere Stellen	46	23,6%
Gesamt	195	100%

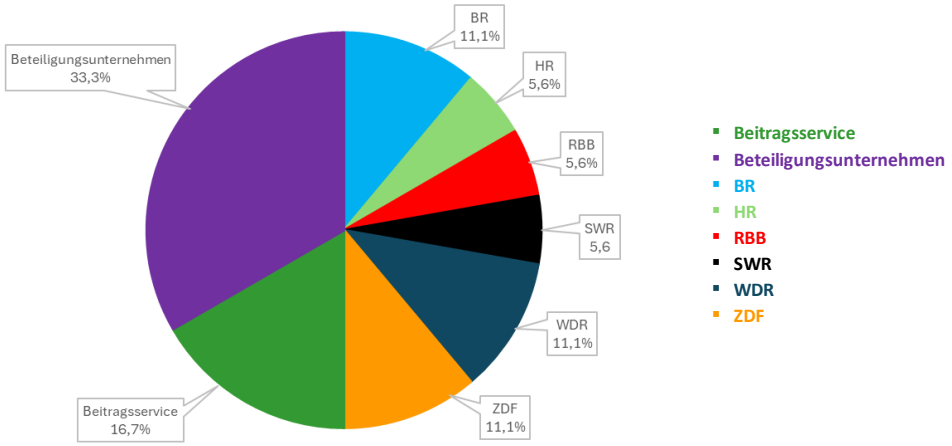


5 Meldungen nach Art. 33 DSGVO

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, also einer Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten führt (vgl. Art. 4 Ziff. 12 DSGVO), ist gemäß Art. 33 DSGVO die Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung zu informieren. Führt eine Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen, kann dies unterbleiben. Seitens des Verantwortlichen ist stets zu prüfen, ob die Voraussetzungen eines meldepflichtigen Vorgangs und der in den Fällen des Art. 34 DSGVO vorgeschriebenen Benachrichtigung davon betroffener Personen vorliegen. Aus Gründen der Risikominimierung ist anzuraten, im Zweifel die Aufsichtsbehörde zu unterrichten.

18 Meldungen zu Datenschutzvorfällen in Rundfunkanstalten und Beteiligungsunternehmen gingen in der Aufsichtsbehörde ein. Die Hälfte der Meldungen war mit einem erhöhten bzw. hohen Risiko zu bewerten und damit notwendig. Wir begrüßen, dass wir bei unklaren Fällen im Zweifel sicherheitshalber informiert wurden. Es fällt allerdings auf, dass drei Rundfunkanstalten keinerlei (selbst nur potenziell risikobehaftete) Datenschutzvorfälle an den Rundfunkdatenschutz-beauftragten gemeldet haben. Dies kann auf ein sehr gutes Funktionieren der Datenschutzprozesse hindeuten oder aber auf nicht in der erforderlichen Weise ausgestaltete Meldeprozesse. Dieses Thema werde ich in den vierteljährlichen Jour fixes näher beleuchten. Denn grundsätzlich kann ich als Aufsicht nur auf Basis der Meldung sicherheitskritischer Aspekte auch übergreifend für alle beaufsichtigten Rundfunkanstalten eine Bewertung vornehmen und diese ggf. kurzfristig informieren bzw. sensibilisieren.

Die Meldungen verteilten sich wie folgt:



	Anzahl		Risikoklassifizierung	
Datenschutzvorfälle	**gesamt**	**Prozent**	**erhöht/hoch**	**gering/nicht vorh.**
Beitragsservice	**3**	16,7%	0	3
Beteiligungsunternehmen	**6**	33,3%	4	2
BR	**2**	11,1%	2	0
Deutschlandradio	**0**	0,0%	-	-
HR	**1**	5,6%	0	1
MDR	**0**	0,0%	-	-
RBB	**1**	5,6%	0	1
SR	**0**	0,0%	-	-
SWR	**1**	5,6%	0	1
WDR	**2**	11,1%	1	1
ZDF	**2**	11,1%	2	0
Gesamt	**18**	**100%**	**9**	**9**

Außerhalb dieser Statistik zu erwähnen ist, dass auch zwei Datenschutzvorfälle gemeldet wurden, für die weder eine Rundfunkanstalt noch ein Beteiligungsunternehmen die Verantwortung trugen. Dabei handelte es sich um eine Betroffeneninformation nach Art. 34 DSGVO durch eine externe Stelle, die uns als Datenschutzvorfall einer Rundfunkanstalt übermittelt wurde. Den Datenschutzbeauftragten des Verantwortlichen haben wir deshalb ein Prozessreview bzgl. der Voraussetzungsprüfung eines meldepflichtigen Vorgangs angeraten.

6 Themen und Schwerpunkte der Aufsicht

Beim Verfassen dieses Berichts hatte ich mich zu fragen, welche Themen berichtenswert sind. Auf die richtige Schwerpunktsetzung kommt es an – ausgehend von meinem Anspruch, einen lesbaren und auch für den Datenschutzlaien interessanten Text zu verfassen. Natürlich muss sich aus dem Bericht auch ergeben, womit ich mich befasst habe und welche Themen besonders wichtig waren und noch sind. Dies vor Augen habe ich die folgende Auswahl getroffen und denke, dass sie einen guten Überblick bietet, der sowohl die Arbeit an einzelnen Themen als auch die Beschäftigung mit übergeordneten Problematiken angemessen beleuchtet.

6.1 Audit Nutzungsmessung

Die Nutzungsmessung in ihren Ausprägungen hatte mich in den vorangegangenen Jahren unter verschiedenen Blickwinkeln immer wieder beschäftigt, sodass es nahelag, sich diesem Thema intensiver zu widmen. Im Tätigkeitsbericht 2023 habe ich zur Zulässigkeit einer statistischen und anonymisierten Nutzungsmessung auch ohne Einwilligung der Nutzerinnen und Nutzer bereits Stellung genommen (siehe dort Kapitel 6.1.1). Die sich bereits de lege lata auf den verfassungsrechtlichen Auftrag der öffentlichen Rundfunkanstalten stützende Argumentation wird sich de lege ferenda durch einen im Entwurf zum Reformstaatsvertrag geschärften Auftrag im Hinblick auf in § 26a MStV-E bezeichnete Leistungsanalysen noch klarer gestalten, wenn dieser Entwurf Geltung entfalten sollte (siehe dazu ausführlich Kapitel 3.5).

Da sowohl die Herleitung der datenschutzrechtlichen Zulässigkeit mit den entsprechenden organisatorischen und technischen Maßnahmen sowie die inhaltliche Ausgestaltung der jeweils eingesetzten Dienste für die Beurteilung einer rechtmäßig gestalteten Nutzungsmessung in den Online-Angeboten der Rundfunkanstalten sowie auch in Apps und Social Media-Angeboten schwer zu überblicken ist und Nutzerinnen und Nutzer in unregelmäßigen Abständen mit Kritik – insbesondere zur einwilligungslosen Ausgestaltung - an mich herantraten, sollte das Thema aus Aufsichtsperspektive näher beleuchtet werden.

Um mir einen Gesamteindruck über alle Nutzungsmessungsaktivitäten in den jeweiligen Online-Angeboten der Rundfunkanstalten zu verschaffen, habe ich im Herbst 2023 begonnen, ein Audit durchzuführen, um zunächst eine Datengrundlage zu erhalten, aus der dann die richtigen Schlüsse im Hinblick darauf gezogen werden sollten, ob die eingesetzten Nutzungsmessungsverfahren den datenschutzrechtlichen Anforderungen und ebenso dem öffentlich-rechtlichen Auftrag entsprechen.

Die Frage der jeweils zugrundeliegenden Rechtsgrundlage war ein zentraler Ansatzpunkt der Untersuchung. Die Erfüllung des Auftrags bedeutet nicht, dass in jeglicher Tiefe und mit jeglichem Anbieter und beliebigen Tools die Nutzung der Angebote gemessen werden darf. Dennoch wird nach meiner Auffassung – wie bereits mehrfach erläutert (siehe zuletzt meinen Tätigkeitsbericht 2023, Kapitel 6.1.1) – für eine anonyme Nutzungsmessung mit dem Ergebnis einer statistischen Auswertung, die sich eben nicht auf eine einzelne Person bezieht oder beziehen lässt, sondern lediglich grundlegende Nutzungs- und Erfolgsdaten erhebt, keine Einwilligung als Rechtsgrundlage benötigt.

Eine statistische Nutzungsmessung ermöglicht es den Rundfunkanstalten, ihrem verfassungsrechtlichen Auftrag nachzukommen und die daraus abgeleitete Verpflichtung umzusetzen, eine zeitgemäße Gestaltung der Telemedienangebote für alle Bevölkerungsgruppen sicher zu stellen (vgl. § 30 Abs. 3 Medienstaatsvertrag). Um dieser Verpflichtung gerecht zu werden, müssen die Rundfunkanstalten wissen, wie ihre Angebote genutzt werden und welche Änderungen im Angebot Auswirkungen auf die Akzeptanz in der Bevölkerung haben. Insofern lässt sich gut begründen, dass dies zum Auftrag gehört, weshalb eine Einwilligung in solcherlei Nutzungsmessung nicht als erforderlich angesehen wird.

Untersucht werden sollte daher auch, ob und welche Methoden die jeweiligen Dienstleister zur Anonymisierung (oder unter bestimmten Voraussetzungen zur Pseudonymisierung) einsetzen, damit das Messergebnis keinen Personenbezug mehr aufweist. Um einerseits einen Überblick über die verwendeten Tools zu gewinnen und andererseits deren rechtskonformen Einsatz und die dabei vorgenommenen Datenverarbeitungen beurteilen zu können, wurden zunächst Fragen entwickelt und in den Rahmen eines thematisch abgestuften Fragenkatalogs eingepasst.

6.1.1 Fragenkatalog und Auswertung

Der Fragenkatalog sollte die wichtigsten Themen benennen und dessen Beantwortung einen Überblick und eine bewertbare Grundlage darüber verschaffen, wie und welche Nutzungsmessungstools tatsächlich eingesetzt werden.

Konkret ging es darum, zunächst sämtliche Websites, Apps, Social Media Angebote, HbbTV und sonstige Angebote der Rundfunkanstalten, für die Nutzungsmessungen durchgeführt werden, zu erfassen und dabei eingesetzte Messmethoden zu benennen. Des Weiteren wurden Zweck und Ziel der Messungen abgefragt sowie die genaue inhaltliche und technische Beschreibung der Messmethoden, die vertragliche Anbindung der Dienstleister und die Rechtsgrundlagen im Hinblick auf den Datenschutz (DSGVO) und TTDSG (jetzt TDDDG). Ein wichtiges Augenmerk lag auch auf den eingesetzten Methoden zur Anonymisierung. Schließlich wurden Fragen nach einer

Datenübermittlung an Drittländer gestellt. Wichtig war ebenso, dass auf die Nutzungsmessung transparent hingewiesen und die datenschutzrechtlichen Besonderheiten so erläutert werden, dass sie leicht zu verstehen und nachvollziehbar sind. Auch dazu wurden Fragen gestellt.

Aufgrund der umfangreichen Daten- und Informationsmengen, die meine Behörde zu den Fragebögen aus den Rundfunkanstalten erreicht haben, war es nicht möglich, eine abschließende datenschutzrechtliche Bewertung der einzelnen Nutzungsmessungstools zu erreichen: Eine technische Untersuchung der tatsächlichen Datenverarbeitungen und insbesondere der häufig eingesetzten Anonymisierungen der personenbezogenen Daten im Messprozess hat sich als undurchführbar erwiesen. Deshalb können die gewonnenen Informationen und Erkenntnisse als Ausgangspunkt für eine weitere Beschäftigung mit diesem Thema aufgefasst werden: Die verantwortlichen Rundfunkanstalten sind aufgefordert, sich intensiv mit dem Thema zu befassen und die offenen Fragen (insbesondere sich selbst) zu beantworten.

6.1.2 Ergebnisse

Zunächst entstand ein Überblick darüber, welche Dienstleister und welche Tools die einzelnen Verantwortlichen jeweils einsetzen. Dabei wurde ersichtlich, welche Tools von allen Verantwortlichen, welche von mehreren Verantwortlichen und welche exklusiv genutzt werden. So kommen einige Rundfunkanstalten mit 2 bis 5 Tools aus, während andere 11 bis 15 Tools im Einsatz haben. Dabei ist jedoch zu beachten, dass die Verantwortlichen teilweise auch Analysen von Drittplattformen miterfassten. Die quantitative Erkenntnis ist besonders im Vergleich und bei der Frage interessant, ob und inwieweit die Nutzung dieser Tools und Messmethoden überhaupt erforderlich ist, und ob sich gemessene und ausgewertete Daten doppeln. Unter dem Gesichtspunkt des Grundsatzes der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO sind Tools, die keinen oder nur einen geringen Mehrwert an Erkenntnis erbringen, gegebenenfalls nicht erforderlich. Die Vielzahl an genutzten Tools hat meine Erwartungen übertroffen.

Erfasst wurden durch den Fragebogen auch sämtliche Angebote, für die die angegebenen Messverfahren eingesetzt werden. Dabei wurde einen Überblick über die Apps und Websites der einzelnen Verantwortlichen gewonnen, genauso wie über die HbbTV-Angebote sowie genutzte Social-Media-Anbieter und das Vorhandensein von digital angebotenen audiovisuellen Inhalten über Drittanbieter (Podcatcher, Spotify, Deezer, IP Radios).

Ein Großteil der verwendeten Tools wird nach den Angaben im Fragebogen unter der Rechtsgrundlage des Funktionsauftrags des öffentlich-rechtlichen Rundfunks gemäß Art. 6 Abs. 1 S. 1 lit. e DSGVO i.V.m. §§ 26, 30 MStV sowie gemäß § 25 Abs. 2 Nr. 2 TTDSG (TDDDG) ohne Einwilligung eingesetzt. Ob sich alle Tools, die von Rundfunkanstalten eingesetzt werden auch tatsächlich unter

die hohen Maßstäbe dieser Rechtsgrundlage fassen lassen, wurde für die Tools im Einzelnen genau geprüft.

Sämtliche Rundfunkanstalten nutzen einheitlich als zentrales Instrument für die Nutzungsmessung der Angebote das Tool von Piano (vormals AT Internet). Aufgrund der Angaben in den Fragebögen und der großen Bedeutung dieses Tools hat meine Behörde daraufhin eine vertiefte Prüfung der Anonymisierungsmethode von Piano begonnen (dazu siehe Kapitel 6.2).

Für die Videostreaming Messung wird von allen Rundfunkanstalten das Tool von Nielsen genutzt. Logfile-Analysen werden mithilfe mehrerer Dienstleister durchgeführt.

Darüber hinaus sind in den Häusern unterschiedliche weitere Tools im Einsatz. Gemessen wird beispielsweise der Erfolg von Werbekampagnen, die Anmeldung zu Newslettern oder Audio-on-Demand/Podcast-Abrufe. Genutzt werden auch Auswertungstools im Zusammenhang mit Social-Media bei denen es sich nach Einschätzung der Verantwortlichen nicht um unmittelbare Nutzungsmessungen handelt, sondern lediglich die Analysen von Drittplattformen genutzt werden. Ob und mit welcher Konsequenz für eine rechtmäßige Nutzung ich diese Einschätzung teile, hängt von weiteren Untersuchungen ab.

6.1.3 Nachfragen

Da die Antworten auf den Fragenkatalog von unterschiedlicher Ausführlichkeit und Qualität waren, wurden teilweise Nachfragen an die Verantwortlichen erforderlich, um eine auch vergleichende Prüfung vornehmen zu können.

Dabei muss festgehalten werden, dass es ausdrücklich nicht der Rechenschaftspflicht der Verantwortlichen (aus Art. 5 Abs. 2, 30 Abs. 2, 58 Abs. 1 DSGVO) genügt, wenn die Aufsichtsbehörde – wie teilweise geschehen – von den Verantwortlichen aufgefordert wird, bei den für einzelne Prozesse konkret zuständigen Personen der Verantwortlichen oder direkt bei den auftragsverarbeitenden Dienstleistern nachzufragen, um Unklarheiten zu beseitigen. Es ist Sache des Verantwortlichen, die Informationen zu beschaffen und der Aufsichtsbehörde zur Verfügung zu stellen. Auch bevor die Aufsichtsbehörde nachfragt, müssen alle erforderlichen Unterlagen (z.B. Vertragsunterlagen) zur Erfüllung von Verpflichtungen aus der DSGVO vorliegen. Verträge und interne Richtlinien müssen gewissermaßen „in der Schublade liegen“, um stets und kurzfristig „rechenschaftsbereit“ zu sein, nur so kann beispielsweise auch fristgerecht auf datenschutzrechtliche Beschwerden und Datenschutzvorfälle reagiert werden.

Aufgrund unserer Nachfragen wurden jedoch erfreulicherweise auch bereits erste Veränderungen/Verbesserungen in puncto Datenschutz und Transparenz durch die Verantwortlichen vorgenommen.

6.1.4 Auditbericht und Ausblick

Die Rundfunkanstalten erhielten nach Abschluss des Audits neben einer allgemeinen Auswertung der gesamten Prüfung eine detaillierte Information sowie Hinweise zu den eingesetzten Tools zur Nutzungsmessung.

Insgesamt hat das Audit aufschlussreiche Erkenntnisse geliefert und gezeigt, dass das Thema Nutzungsmessung datenschutzrechtlich nach wie vor schwierig und im Detail nicht unumstritten ist.

Eine vertiefte Befassung mit dem Thema hat sich jedenfalls und zusammenfassend als fruchtbar und sinnvoll erwiesen, da es einen Blick auf die unterschiedliche Handhabung in den Rundfunkanstalten ermöglicht. Dies ist grundsätzlich nicht zu beanstanden, bedurfte jedoch im Hinblick auf die datenschutzrechtliche Zulässigkeit einer genauen Analyse.

Es zeigte sich in der Auswertung, dass es häufig nicht genügt, sich auf die vertraglichen Grundlagen zu verlassen, sondern bei Unklarheiten im Einzelfall Gespräche mit den Dienstleistern geführt werden müssen, um diese aufzulösen. Nur so kann eine rechtmäßige und rechtssichere Nutzungsmessung gewährleistet werden. Das wiederum ist auch für das Vertrauen der Betroffenen – also der Nutzerinnen und Nutzer der digitalen Angebote des öffentlich-rechtlichen Rundfunks – von nicht unerheblicher Bedeutung.

Ich habe im Auditbericht zudem Empfehlungen für Maßnahmen ausgesprochen, um eine rechtmäßige Nutzungsmessung durch die Verantwortlichen zu gewährleisten. Ich haben den Verantwortlichen empfohlen, sämtliche Datenschutzerklärungen auf die ordnungsgemäße Beschreibung der Nutzungsmessungs-Tools hin zu überprüfen. Dabei soll das Augenmerk darauf gerichtet werden, dass die zugrunde gelegten Rechtsgrundlagen vollständig abgebildet und die damit ggf. verbundenen Anonymisierungsmethoden geprüft werden. Rechtlich und technisch muss die jeweiligen Funktionsweise von den Verantwortlichen durchdrungen werden, andernfalls kann kein Einsatz erfolgen. Im Rahmen der Untersuchung zeigte sich stellenweise, dass Tools auch dann eingesetzt wurden, wenn den Verantwortlichen relevante Informationen der Dienstleister fehlten.

Aufgabe als Aufsichtsbehörde ist es in diesem Zusammenhang, unterschiedliche Handhabungen der Verantwortlichen zu hinterfragen, auf diese hinzuweisen, hinsichtlich der erforderlichen rechtlichen Grundlagen zu sensibilisieren und besonders problematische Themen aufzugreifen und

gegebenenfalls Anpassungen und Verbesserungen herbeizuführen. Dies ist als gelungen einzustufen.

Das Audit war in diesen Belangen von einem hohen Erkenntnisgewinn geprägt und führte bereits zu Optimierungen sowie in bestimmten Fällen zu einem Hinterfragen und Prüfen der Erforderlichkeit einzelner Tools. Durch die Sensibilisierung der Rundfunkanstalten ist zu erwarten, dass in Zukunft ein besseres Gespür für die Anforderungen an einen rechtmäßigen Einsatz von Nutzungsmessungstools besteht.

Die Vielfältigkeit und schiere Anzahl der eingesetzten Messmethoden, ebenso die technische Komplexität der verwendeten Software und nicht zuletzt die unterschiedlichen Begriffe, die zur Beschreibung der einzelnen Datenkategorien und Messpunkte verwendet wurden, haben es äußerst schwierig gemacht, mit den zur Verfügung stehenden Ressourcen und Kapazitäten meiner Behörde alle Fragen zu beantworten und die Untersuchung unter dem Blickwinkel einer umfassenden rechtlichen und technischen Bewertung aller Tools abzuschließen. Dessen ungeachtet bin ich mit dem Ergebnis sehr zufrieden, denn die Erhebung und Analyse erlaubt es, sich kritisch mit dem Thema Nutzungsmessung auseinanderzusetzen und ermöglicht es den verantwortlichen Rundfunkanstalten, genauere Anforderungen zu formulieren und den Nutzen der Messung mit den Datenschutzanforderungen ins Verhältnis zu setzen.

6.2 Nutzungsmessung durch Piano Analytics

Im letzten Tätigkeitsbericht für das Jahr 2023 habe ich unter Kapitel 6.1.2 zum Audit der Nutzungsmessung in den Online-Angeboten angekündigt, mich mit der Anonymisierungsmethode beim Einsatz des Tools von Piano Analytics beschäftigen zu wollen. Im Berichtsjahr habe ich das Thema weiterverfolgt und bin zunächst an Piano Analytics mit verschiedenen Fragen herangetreten, um letztendlich die Frage zu klären, ob aus Sicht der Rundfunkanstalten von einer anonymisierten Nutzungsmessung ausgegangen werden kann.

Insbesondere wurde gefragt, welche Daten tatsächlich im Rahmen dieser statistischen Nutzungsmessung verarbeitet werden und wie die Anonymisierungsmethoden des Dienstleisters aussehen. Ebenso habe ich um Einschätzung darum gebeten, ob die dort verarbeiteten IDs ggf. als personenbezogen angesehen werden.

Diese Antworten auf diese Fragen habe ich sodann mit Schreiben vom 08.08.2024 den Rundfunkanstalten vorgelegt und um eine Stellungnahme dazu gebeten. Die Rundfunkanstalten haben, vertreten durch die ARD-Geschäftsführung, mit einer gemeinschaftlichen Stellungnahme am

14.10.2024 geantwortet. Die in der RDSK abgestimmte Antwort darauf erfolgte dann am 17.12.2024.

Dieser Tätigkeitsbericht ist gewiss nicht die Stelle, um ins Detail zugehen, jedoch sollen die wesentlichen Diskussionspunkte hier kurz dargestellt werden.

Sowohl die Antworten von Piano Analytics als auch die Stellungnahme der Rundfunkanstalten konnten nicht alle Fragen vollständig klären. Insbesondere die Fragen nach dem Personenbezug und der Interpretation des Begriffs „Anonymisierung“ erweisen sich nach wie vor als schwierig. Nicht umsonst beschäftigt sich die DSK und damit die staatlichen Datenschutzaufsichtsbehörden im Jahr 2025 schwerpunkmäßig mit Fragen zur Anonymisierung von Daten.

Ich habe mich in meiner Antwort auch unter Bezugnahme auf den Tätigkeitsbericht des Jahres 2023, (dort Kapitel 3.4.1) dergestalt geäußert, dass eine relative Anonymisierung in Ansehung des Auftrags des öffentlich-rechtlichen Rundfunks als ausreichend erachtet werden kann. Die Rundfunkanstalten sind aber dennoch aufgefordert, eine Risikoabschätzung in Bezug auf diese relative Anonymisierung und den damit nicht gänzlich auszuschließenden Personenbezug vorzunehmen. Es geht darum, Risiken im Hinblick auf die Identifizierbarkeit der User unter jeglichen Gesichtspunkt zu analysieren und darzustellen.

In den Blick genommen und auch in die Entscheidung einbezogen wurde der Entwurf des Reformstaatsvertrages (siehe hierzu auch Kapitel 3.5), nach dem auch Leistungsanalysen und die Erhebung der quantitativen und qualitativen Nutzung der Angebote durch Zielgruppen zu den Pflichten des öffentlich-rechtlichen Rundfunks gehören. Nach meiner und der Auslegung der RDSK kann eine dementsprechende Verarbeitung personenbezogener Daten zur Erfüllung des dann detailliert ausgestalteten Auftrags im Einzelfall und nach genauer Prüfung erforderlich sein: Im Hinblick darauf, dass möglicherweise eine statistische Nutzungsmessung dem Auftrag nicht mehr genügt, sondern die Nutzung der Angebote feingranularer unter Berücksichtigung von Quoten, Abrufzahlen, Nutzungsdauer und angestrebten Zielgruppen nachgewiesen werden muss, sind die dafür erforderlichen personenbezogenen Daten rechtmäßig zu verarbeiten, ohne dass es auf eine Einwilligung der Nutzenden ankäme.

Der Gesetzgeber steht nach meiner Interpretation auf dem Standpunkt, dass Daten von Nutzenden verarbeitet werden dürfen, soweit dies zur Erfüllung des Auftrags erforderlich ist. Dieser offensichtliche gesetzgeberische Wille hat mich dazu veranlasst, die aktuell vorgenommene Nutzungsmessung durch den öffentlich-rechtlichen Rundfunk auch unter diesen Blickwinkel zu bewerten, sodass eine Untersagung der einwilligungsfreien Nutzungsmessung schon aus diesem Grund als unverhältnismäßig angesehen wurde. Klar ist aber auch, dies entbindet die verantwortlichen Rundfunkanstalten nicht davon, sowohl im Hinblick auf die Datenminimierung als auch auf die zu ergreifenden technischen und organisatorischen Maßnahmen sicherzustellen, dass

die Nutzungsmessung bis auf weiteres ohne Personenbezug abläuft und zumindest unter Zugrundelegung des relativen Anonymisierungsbegriffs als anonym angesehen werden kann.

Mit dieser Bewertung haben wir uns im Kreis der RDSK nicht leichtgetan, denn eine Beurteilung der einzelnen Datenarten und Kategorien war nicht einfach. Dennoch hat sich der Eindruck verfestigt, dass die Rundfunkanstalten das Thema ernst nehmen und sich vertieft mit der Materie auseinandersetzen. Dennoch – und darauf werde ich stets hinweisen – sind die Rundfunkanstalten regelmäßig verpflichtet, das Risiko für die informationelle Selbstbestimmung beim Einsatz solcherlei Nutzungsmessungstechniken zu bewerten und im Blick zu behalten. Ggf. werden die Vorschriften des Reformstaatsvertrages an der einen oder anderen Stelle eine Neubewertung notwendig machen, von einem sorgfältigen Umgang mit den Daten der Nutzerinnen und Nutzer von Angeboten der Rundfunkanstalten entbindet dies indes nicht.

6.3 Einführung lineare Nutzungsmessung HbbTV

Ende Januar 2024 setzte das ZDF eine einwilligungsbasierte neue Nutzungsmessung um, die es ermöglichte, auch bei HbbTV[16]-fähigen Fernsehgeräten das lineare Nutzungsverhalten für die Angebote ZDF, ZDFinfo und ZDFneo sowie die HbbTV-Applikationen ZDFmediathek, ZDFtivi und ZDFheute zu messen. In diesem Rahmen kam es zu unerwarteten Herausforderungen, die sich auch in bei uns eingehenden Beschwerden widerspiegelten.

Durch ein technisches Problem konnte das für die Einwilligung vorgesehene Cookie-Banner auf einigen Geräten nicht geschlossen werden – weder durch Erteilung der Einwilligung noch durch Ablehnung. Auch wenn das Problem im Ausgangspunkt technischer Natur war und letztlich gelöst werden konnte, musste geklärt werden, ob in einem bestimmten Zeitraum eine Nutzungsmessung ohne wirksame Einwilligung erfolgt sein könnte, z.B., indem man das Cookie-Banner nur durch eine „unfreiwillige Einwilligung“ hätte verlassen können. Dies war aber zu keinem Zeitpunkt der Fall.

Auch grundsätzliche Bedenken zur Rechtmäßigkeit des „Trackings“ durch das ZDF wurden laut. Die erforderlichen bzw. freiwilligen Datenverarbeitungen wurden jedoch nach geltendem Recht umgesetzt und transparent kommuniziert. Im Menüpunkt „Datenschutzeinstellungen“ in der jeweiligen App bzw. beim Klick auf die Kachel „Datenschutzeinstellungen“ in der HbbTV-Startleiste werden die Datenverarbeitungen in verschiedene Kategorien unterteilt und erläutert:

- Die erste Kategorie betrifft „technisch erforderliche“ Datenverarbeitungen. Diese lassen sich nicht abwählen, da sie die grundlegenden Funktionen des Angebots gewährleisten (hierzu

[16] Hybridfernsehen (HbbTV) verbindet klassisches lineares Fernsehen mit dem Internet.

zählen z.B. die Einstellungen im Videoplayer, der Login-Status, oder die Datenschutzeinstellungen).

- Die zweite Kategorie „erforderliche Erfolgsmessung“ ist ebenfalls nicht abwählbar. Die statistische Nutzungsanalyse, die in anonymisierter Form erfolgt, dient dem Zweck, das Telemedienangebot laufend und zeitgemäß zu optimieren. Die Nutzungsmessung erfolgt daher aus rein publizistischen und nicht etwa aus kommerziellen Zwecken. Rechtlicher Hintergrund ist die Erfüllung des verfassungsrechtlichen Programmauftrags des öffentlich-rechtlichen Rundfunks (siehe hierzu Kapitel 6.1).
- Die in der dritten Kategorie benannte „zusätzliche Erfolgsmessung“ betrifft die neu eingeführte Nutzungsmessung im linearen Fernsehen und ist nur bei internetfähigen Fernsehgeräten möglich. Sie wird nur mit vorheriger Zustimmung vorgenommen. Dabei können die Nutzungsdaten für des ZDF je Gerät mit den Nutzungsdaten anderer Sender, die vom gleichen Dienstleister erfasst werden, über eine anonymisierte Geräte ID zusammengeführt werden. Eine Rückverfolgbarkeit und damit ein Personenbezug ist nach Auskunft des ZDF ausgeschlossen. Wenn im Cookie-Banner oder in den Einstellungen „Abwählen“ geklickt wird, findet diese zusätzliche Erfolgsmessung nicht statt.
- Die vierte Kategorie „Personalisierung“ führt bei Zustimmung zu erweiterten personalisierten Funktionen (z.B. „Weiterschauen“) und ist ohne Einwilligung nicht möglich. Wenn im Cookie-Banner oder in den Einstellungen „Abwählen“ geklickt wird, erfolgt keine Personalisierung der Inhalte des ZDF.

Da die zusätzliche Erfolgsmessung in rechtskonformer Weise einem Einwilligungsvorbehalt unterstellt ist, begegnet die damit einhergehende Datenverarbeitung keinen grundsätzlichen Bedenken. Eine vertiefte Prüfung bleibt ggf. einem späteren Zeitpunkt vorbehalten.

6.4 Künstliche Intelligenz

Am Thema Künstliche Intelligenz kam im Jahr 2024 niemand vorbei, der sich mit Datenschutz beschäftigt. Wie in der Vorausschau im Tätigkeitsbericht 2023 (siehe dort Kapitel 6.2.) schon vermutet, spielte im Berichtsjahr 2024 das Thema eine bedeutende Rolle für die Rundfunkanstalten und folglich ebenso für die Datenschutzaufsicht. Denn wo KI im Einsatz ist, fließen Daten, und einige davon sind personenbezogen.

Bereits die Prüfung, ob Personenbezug anzunehmen ist, stellt in der Praxis eine enorme Herausforderung dar, von deren Feststellung allerdings die rechtliche Behandlung in bedeutendem Maße abhängt. Die KI-Verordnung (siehe Kapitel 3.2) reguliert zwar den Einsatz von KI aus dem Blickwinkel einer rechtlichen Risikosphäre, hat aber nicht in erster Linie das Datenschutzrecht vor

Augen. Die DSGVO bleibt in vollem Umfang anwendbar und muss daher bei Herstellung, Training und Einsatz von KI-Modellen und KI-Systemen beachtet werden.

In den Rundfunkanstalten wird an eigenen KI-Systemen gearbeitet, teilweise sind anstaltseigene geschlossene KI-Systeme bereits im Einsatz. Die Vernetzung auch zwischen den Rundfunkanstalten nimmt zu, so gibt es beispielsweise ein KI-Netzwerk in der ARD, regelmäßige Informations- und Diskussionsrunden über verschiedene Kanäle sowie KI-Projekttage und KI-Räte in den einzelnen Rundfunkanstalten. Auch wenn der Innovationsgeist in Produktion und Redaktion häufig im Vordergrund steht, so hängt der Einsatz von der Überwindung rechtlicher Hürden ab. Wie bereits im Kapitel 3.2 erwähnt, muss die KI-Kompetenz entsprechend Art. 4 KI-VO nachgewiesen werden. Die Verantwortlichen müssen dies durch Schulungen und Zertifikate, wie beispielsweise „KI-Führerscheine“ umsetzen. Dabei sollte die datenschutzrechtliche Kompetenz beim Thema KI in den Fokus rücken.

Um die datenschutzrechtliche Unsicherheit bezogen auf den Einsatz von KI im öffentlich-rechtlichen Rundfunk abzubauen, habe ich gemeinsam mit der RDSK im August 2023 eine Orientierungshilfe erarbeitet, die erste Eck- und datenschutzrechtliche Anknüpfungspunkte hinsichtlich des Einsatzes von Künstlicher Intelligenz bieten sollte. Das Papier war zunächst als interne Orientierungshilfe gedacht und in der ersten Version noch nicht veröffentlicht worden. Durch das hilfreiche Feedback aus den Rundfunkanstalten, insbesondere von den internen Datenschutzbeauftragten, wurde die Orientierungshilfe zwischenzeitlich in einer zweiten Version anwendungsfreundlicher gestaltet und in der aktuellen Version 2.1. im September 2024 wiederum, auch bezugnehmend auf die Regelungen der in der Zwischenzeit in Kraft getretenen KI-Verordnung, nachgeschärft und auf der RDSK-Website veröffentlicht[17] (zu den Inhalten der Orientierungshilfe vgl. Kapitel 9.2.1).

6.5 Befragung zu Onboarding und Schulung

Der reflektierte Umgang mit personenbezogenen Daten durch Beschäftigte[18] ist sicher zu stellen; zur Erfüllung dieser Pflicht sind Onboarding- und Schulungsprozesse basierend auf den geltenden Datenschutzvorschriften notwendig. Um mir einen Überblick zu den diesbezüglich vorgesehenen und umgesetzten Prozessen und Maßnahmen zu verschaffen, habe ich im Zeitraum

[17] https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/orientierungshilfen/orientierungshilfe-zum-datenschutzkonformen-einsatz-von-ki-im-oeffentlich-rechtlichen-rundfunk

[18] Unter den Begriff Beschäftigte werden alle Beschäftigten subsummiert, die für die befragten Verantwortlichen tätig sind, dies können im Detail sein: Arbeitnehmende in Festanstellung oder Ausbildung, Praktikanten/Praktikantinnen, freie Mitarbeitende, Volontäre/Volontärinnen, Aushilfen und Leiharbeitende.

November/Dezember 2024 eine Befragung an die durch uns beaufsichtigten Verantwortlichen[19] gerichtet. Diese bezog sich auf Maßnahmen

- zur Erfüllung der Informationspflichten und Verpflichtung auf die Wahrung zur Vertraulichkeit personenbezogener Daten/das Datengeheimnis im Rahmen des Onboardings neuer Beschäftigter sowie
- zur Gestaltung der Datenschutz-Schulungsprozesse.

Die Antworten wurden uns fristgerecht mitgeteilt, so dass wir im Folgejahr 2025 die Ergebnisse bewerten und nebst Handlungsempfehlungen an die Verantwortlichen übermitteln können. In diesem Rahmen werden wir eine Rückmeldung zum Umgang mit unseren Handlungsempfehlungen und zu geplanten und umgesetzten Maßnahmen erbitten. Weitere Informationen zum Ergebnis der Untersuchung sind dem Tätigkeitsbericht zum Jahr 2025 vorbehalten.

6.6 Geplantes Audit von Nachrichten-Apps

Im Rahmen der Auftragserfüllung bietet der öffentlich-rechtliche Rundfunk Apps zur Verwendung insbesondere auf mobilen Endgeräten an. Bei der Nutzung von Apps verarbeiten diese personenbezogenen Daten oder haben Zugriff darauf und kommunizieren mit diversen Diensten im Internet. Vor diesem Hintergrund muss die Datenverarbeitung gegenüber den Nutzenden stets transparent und unter Berücksichtigung der datenschutzrechtlichen Vorgaben erfolgen.

Da mich seit Amtsübernahme Fragen und auch Beschwerden zu der Umsetzung und Transparenz von Datenschutzhinweisen in Apps einzelner Rundfunkanstalten erreicht hatten, plante ich im Berichtsjahr die Datenverarbeitung von Apps der von mir beaufsichtigten Rundfunkanstalten genauer in Augenschein nehmen. Ziel war es, je Rundfunkanstalt eine Nachrichtenapp sowohl aus dem Apple App Store als auch dem Google Playstore zu überprüfen. Hier sollte der Fokus auf einer technischen Analyse der tatsächlich stattfindenden Datenverarbeitung im Rahmen der App-Nutzung liegen, deren Ergebnisse in die Überprüfung der Umsetzung der Transparenzanforderungen der zugehörigen Datenschutzhinweise nach Art. 12 ff. DSGVO einbezogen werden sollten.

[19] Mit dem Begriff Verantwortliche (bei übergreifender Verwendung in maskuliner Form) sind im Sinne einer einheitlichen Befragung sowohl die beaufsichtigten Rundfunkanstalten als auch die Körperschaft Deutschlandradio und der Beitragsservice als Gemeinschaftseinrichtung gemeint.

Um die Unabhängigkeit der technischen Analyse zu gewährleisten war geplant, damit einen externen Dienstleister zu beauftragen. Es konnten hier zwei potenzielle Partner in die engere Auswahl genommen werden.

Verschiedene Entwicklungen brachten das Audit-Vorhaben zunächst leider zum Stillstand. Dazu gehört zunächst das mir für solcherlei Aufgaben zur Verfügung stehende Budget, das in keinem Verhältnis zu den Kosten einer externen Beauftragung der Analyse steht. Als vergleichsweise kleine Aufsichtsbehörde mit insgesamt vier Beschäftigten sind wir in die technische Infrastruktur der beaufsichtigten Rundfunkanstalten eingebunden, jedoch steht mir kein eigenes IT-Personal zur Verfügung, das ich mit einer unabhängigen technischen Analyse beauftragen könnte.

Im Tätigkeitsbericht 2023 des Hamburgischen Beauftragten für Datenschutz und Informationssicherheit wurde darauf verwiesen, dass dort bereits App-Analysen umgesetzt worden sind. Also habe ich mich im Sinne der Amtshilfe und Unterstützung an die dort sehr entgegenkommenden Kollegen gewandt. Im Ergebnis ist es zwar nicht möglich, direkt deren Analyse-Lösung zu nutzen, jedoch bin ich zuversichtlich, dass meine Behörde mit deren angebotener Unterstützung zukünftig ein eigenes, überschaubares IT-Labor aufsetzen können wird.

Auch weil sich die App-Angebote bedingt durch die KEF-Anforderungen aktuell kontinuierlich verändern, war ein Pausieren des Audits der richtige Schritt. Die „App-Landschaft“ der beaufsichtigten Rundfunkanstalten befindet sich durch Effizienz- und Optimierungsstrategien in einem Wandel. Erst wenn diese Umstrukturierungsprozesse abgeschlossen sind, ist eine Auditierung von Apps wieder ein zielführendes Unterfangen. Und bis zu diesem Zeitpunkt planen wir auch, ein eigenes IT-Labor für diese Zwecke aufzubauen.

6.7 Medienprivileg

Als Medienprivileg wird die Bereichsausnahme für die insoweit privilegierten Medien von den datenschutzrechtlichen Anforderungen bezeichnet. Während auf der einen Seite die informationelle Selbstbestimmung steht (aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), rückt beim Journalismus auf der anderen Seite das öffentliche Informationsinteresse, die Freiheit von Presse und Rundfunk (Art. 5 GG) und damit das Veröffentlichungsinteresse in den Vordergrund.

6.7.1 Rechtsgrundlagen und Anwendbarkeit des Medienprivilegs

Die §§ 12 Abs. 1, 23 Abs. 1 Medienstaatsvertrag (MStV) legen im Rahmen der Öffnungsklausel des Art. 85 Abs. 1 DSGVO fest, welche datenschutzrechtlichen Vorgaben der DSGVO für die

journalistische Datenverarbeitung gelten. Art. 85 Abs. 2 DSGVO skizziert bereits die Passagen der DSGVO, für die die Mitgliedstaaten Ausnahmen und Abweichungen vorsehen sollen, die sich in den §§ 12 Abs. 1 und 23 Abs. 1 MStV wiederfinden.

Die Anwendbarkeit der DSGVO wird danach weitgehend ausgeschlossen. Uneingeschränkt gilt jedoch das Datengeheimnis, also die Untersagung, die zu journalistischen Zwecken verarbeiteten personenbezogenen Daten zu anderen Zwecken zu verarbeiten. Integrität und Vertraulichkeit der Daten müssen außerdem gewährleistet werden.

Entscheidend für die Anwendung des Medienprivilegs ist also die Einordnung der Datenverarbeitung unter den Begriff „journalistische Zwecke“[20]. Nach dem EuGH (Urt. v. 14.02.2019 – C 345/17 - Buivids) ist ein Zweck journalistisch, wenn Informationen, Meinungen oder Ideen in der Öffentlichkeit verbreitet werden und damit ein Beitrag zur öffentlichen Meinungsbildung geleistet wird, gleich mit welchem Übertragungsmittel. Als journalistische Herangehensweise wird ein Mindestmaß an eigener inhaltlicher Bearbeitung der bereitgestellten Informationen vorausgesetzt (BGH, Urt. V. 12.12.2021 – VI ZR 488/19). Neben Medienunternehmen und Rundfunkanstalten können damit auch einzelne Blogger oder Betreiber von Social-Media-Kanälen journalistische Zwecke verfolgen und so unter das Medienprivileg fallen.

Keine journalistischen Zwecke werden gesehen bei der Datenverarbeitung für den Rundfunkbeitragseinzug, Akquise von Abonnenten, kommerzieller Weitergabe an Dritte, z.B. für Werbezwecke oder an Suchmaschinen. Wenn eine Datenverarbeitung vorliegt, die nicht journalistischen Zwecken dient, muss für eine rechtmäßige Verarbeitung eine Rechtsgrundlage nach Art. 6 DSGVO gefunden werden.

Für die Datenverarbeitung im journalistischen und redaktionellen Kontext in den Rundfunkanstalten greift somit das Medienprivileg. Viele Beschwerden, die beispielsweise eine Erkennbarkeit der betreffenden Person in journalistischen Beiträgen monieren, weil eine Einwilligung fehle, lassen sich mit Verweis auf das und Erläuterung des Medienprivilegs beantworten. Unbenommen bleibt die persönlichkeitsrechtliche Komponente, die jedoch nicht von der Datenschutzaufsichtsbehörde zu prüfen ist. Naturgemäß eröffnen sich aber auch Grenzbereiche, die einerseits zwar Bezug zur journalistischen Tätigkeit der Rundfunkanstalten aufweisen, andererseits im Schwerpunkt selbst aber nicht journalistischer Art sind. Bereits im Tätigkeitsbericht 2023, Kapitel 6.3.2 ff., habe ich bestimmte Grenzbereiche beleuchtet, die mich im Kontext des Rundfunkdatenschutzes beschäftigt haben.

[20] Dazu auch bereits mein Vorgänger im Amt: Binder, Rechtsfragen zum Datenschutz und zur Datenschutzaufsicht im Rundfunk – Teil 1, AfP 2022, 93-100 (96 ff.)

Auch in diesem Bericht möchte ich – wenn auch nicht sehr ausführlich – auf Teilaspekte eingehen.

6.7.2 Kommentare auf Facebook-Kanal

Mich erreichte eine Beschwerde zu einem abgelehnten Auskunftsbegehren zu auf Facebook getätigten Kommentaren des Betroffenen unter Beiträgen eines von einer Rundfunkanstalt betriebenen Facebook-Kanals.

Kommentare von Nutzern unter journalistische Beiträge unterfallen jedoch ebenso wie die Beiträge selbst dem Medienprivileg. Der Sinn liegt auch hier darin, das Recht auf den Schutz personenbezogener Daten mit der Presse- und Rundfunkfreiheit in Einklang zu bringen.

Da der Begriff der journalistischen Datenverarbeitung weit auszulegen ist, sind Kommentarfunktionen im Rahmen eines journalistischen Beitrages nach meiner Auffassung zweifelslos darunter zu fassen. Daher erstreckt sich das als Auskunftsanspruch ausgestaltete Betroffenenrecht nach Art. 15 DSGVO nicht auf die personenbezogenen Daten innerhalb der von Facebook-Nutzern geschriebenen Kommentare.

6.7.3 Subsidiäre Aufsichtszuständigkeit

Unter Kapitel 2.2 dieses Berichtes habe ich von einer Presseanfrage berichtet und ebenso von der subsidiären Aufsichtszuständigkeit des Rundfunkdatenschutzbeauftragten in solchen Angelegenheiten[21]. Auf eine Besonderheit wurde hingewiesen, die sich in verschiedenen Rechten von Personen zeigen, die eine Persönlichkeitsrechtsverletzung (außerhalb des Datenschutzrechts) durch die Berichterstattung erlitten haben. Auch dies ist Ausfluss des Medienprivilegs, der der Datenschutzaufsicht eben keine Aufsicht über die direkt medienprivilegierten Daten zuweist, sondern nur hinsichtlich solcher Daten, die nach der Feststellung einer Persönlichkeitsrechts-Beeinträchtigung als Grundlage der Berichterstattung weiterhin verarbeitet werden.

Dies scheint auch sachgerecht, da hier der Schutzbereich der Rundfunkfreiheit zumindest teilweise verlassen wird. Im Ergebnis geht es um Auskunftsrechte zu den einer Berichterstattung zugrunde liegenden Daten. Aber auch in dieser Konstellation kann die Auskunft verweigert werden, wenn auf besonders schützenswerte Personen wie bspw. Informanten geschlossen werden kann oder die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde[22].

[21] Vgl. § 12 Abs. 2, 3; § 23 Abs. 2, 3, MStV
[22] Siehe § 12 Abs. 3 Ziff 1.-3. MStV

Ebenso besteht u.U. das Recht auf Berichtigung unrichtiger personenbezogener Daten im Datensatz oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang.

6.7.4 Correctiv - Wem gehört die Stadt ?

Wie an verschiedenen Stellen dargestellt, erreichen mich regelmäßig Beschwerden, die ich aufgrund der Medienprivilegierung der Berichterstattung zurückzuweisen habe. Dies sind in den allermeisten Fällen Sachverhalte, in denen Betroffene ihre Darstellung in einem journalistischen Beitrag oder in der Berichterstattung als nicht datenschutzkonform ansehen und daher Beschwerde einlegen.

Ein insoweit interessanter Fall erreichte mich beim Bayerischen Rundfunk. Im Rahmen der Recherche zur Aktion „Wem gehört die Stadt?“ waren Mieter in München aufgerufen, Angaben zu ihrem Vermieter an den BR zu melden. Der Beschwerdeführer – seiner Aussage nach Eigentümer zweier Wohnungen in München – ging davon aus, dass Daten zu seiner Person im Rahmen dieser Aktion an den Bayerischen Rundfunk gemeldet worden waren.

Der interne Datenschutzbeauftragte des BR hatte in Reaktion auf ein Auskunftsersuchen des Beschwerdeführers bereits darauf verwiesen, dass diese personenbezogenen Daten zu journalistischen Zwecken verarbeitet worden seien, sodass das Medienprivileg greife. Folgerichtig hatte er verdeutlicht, dass ein datenschutzrechtlicher Auskunftsanspruch im Hinblick auf diese Daten ausscheide und eine Auskunft verweigert.

Der Beschwerdeführer stand auf dem Standpunkt, dass das Medienprivileg in dem Fall keine Anwendung finde, da er als Person nicht Teil der Berichterstattung sei. Er argumentierte, dass mit dem Auskunftsersuchen die journalistische Arbeit nicht eingeschränkt sei.

Ich habe die Beschwerde geprüft und bin zu dem Ergebnis gekommen, dass entgegen der Argumentation des Beschwerdeführers sehr wohl das Medienprivileg einschlägig war. Insbesondere musste berücksichtigt werden, dass der Begriff des Journalismus weit auszulegen ist und sich das Privileg nicht nur auf Personen und deren Datenverarbeitung bezieht, über die direkt berichtet wird oder die in Beiträgen sichtbar sind, sondern auch auf die der Berichterstattung zugrunde liegenden oder damit zusammenhängenden Tätigkeiten. Der gesamte Prozess von der Recherche bis zur Archivierung ist vom Medienprivileg umfasst und kann so die Rundfunkfreiheit effektiv schützen.

6.8 Erfüllung Informationspflichten gegenüber Beschäftigten

Seitens des Beitragsservice wurde ich mit einem Fall konfrontiert, auf den die DSGVO oder andere Vorschriften auf den ersten Blick kaum passen. Es ging konkret um die Frage, was aus Datenschutzsicht zu beachten ist und welche Informationspflichten den Verantwortlichen treffen,

wenn nach internen Ermittlungen wegen des Verdachts von strafbaren Handlungen dieser Verdacht nicht bestätigt werden kann. Ein wahrscheinliches Anwendungsszenario sind Meldungen im Sinne des Hinweisgeberschutzgesetzes.

Grundsätzlich gilt, dass – auch wenn personenbezogenen Daten nicht bei der betroffenen Person erhoben werden – verschiedene Informationen mitzuteilen sind, vgl. Art. 14 DSGVO.

Es liegt auf der Hand und ist auch gesetzlich in Art. 14 Abs. 5 lit. b DSGVO so vorgesehen, dass die beschuldigte Person während der Ermittlungen über die Datenverarbeitung nicht zu informieren ist, wenn der Erfolg der Ermittlungen dadurch gefährdet würde. Wenn sich aber nach Abschluss der Ermittlungen herausstellt, dass keine Beweise für eine Verfehlung zu erbringen sind, ist fraglich, ob die betroffene Person nachträglich über die durchgeführten Ermittlungen und die dazu verarbeiteten Daten informiert werden muss oder ob es ggf. ausreicht, allgemein über die Ermittlungen zu informieren.

Ich habe mich intensiv mit der Frage auseinandergesetzt und zunächst festgestellt, dass sich aus dem Wortlaut des Art. 14 Abs. 5 DSGVO nicht eindeutig herleiten lässt, dass eine Nachholung der während der Ermittlung ausgeschlossenen Informationspflicht erfolgen muss, nach dem die Gründe für diesen Ausschluss entfallen sind – im hier betrachteten Fall also der Abschluss der Ermittlungen und der Entlastung des Mitarbeitenden.

Im Ergebnis habe ich die Auffassung vertreten, dass die Informierung des Beschuldigten nach Ende der Ermittlungen zu einer Verdachtsmeldung nicht dauerhaft durch Art. 14 Abs. 5 lit. b DSGVO gehindert ist, und nur eine Nachholung der Informationen dem Sinn und Zweck der DSGVO, nämlich dem effektiven Schutz des Grundrechts auf informationelle Selbstbestimmung, gerecht wird.

Eine strenge Verpflichtung zur nachträglichen Information des Betroffenen ergibt sich nicht ausdrücklich aus der DSGVO, jedoch müssten diese Informationen dann bereitgestellt werden, wenn sich dies nach einer Interessenabwägung als verhältnismäßig herausstellt. Insofern bedarf es einer Einzelfallbetrachtung. Es ist auch während der Untersuchung oder Ermittlung in den Blick zu nehmen, ob die Unterrichtung der (ehemals) Beschuldigen die Fähigkeit eines Verantwortlichen zur wirksamen Untersuchung des Vorwurfs oder zur Sammlung der erforderlichen Beweise gefährden würde. Dann kann die Information der beschuldigten oder ehemals beschuldigten Person so lange aufgeschoben werden, wie diese Gefahr besteht.

Ich habe dem Beitragsservice mitgeteilt, dass die Monatsfrist aus Art. 14 Abs. 3 lit. a DSGVO für eine nachträgliche Informationspflicht als zeitliche Orientierung gilt. Allerdings ist zu beachten, dass auf den Umstand des Wegfalls der hindernden Gründe nach Art. 14. Abs. 5 lit. b DSGVO abgestellt werden muss. Wichtig ist ebenso, dass bei der nachträglichen Information des letztendlich zu Unrecht Beschuldigten die Identität einer ggf. meldenden Person ausgenommen sein muss. Sollte etwas anderes gelten, müsste sich dies unmittelbar aus dem Datenschutzrecht ergeben.

Eine Vorabinformation sämtlicher Beschäftigten in allgemeiner Form über mögliche Ermittlungen im Rahmen von Sonderprüfungen genügt meines Erachtens nicht dem Grundgedanken des Art. 14 DSGVO, denn dieser stellt auf die direkt betroffene Person und deren personenbezogene Daten ab.

Ich halte dieses Ergebnis für zutreffend, da es einem angemessenen Ausgleich zwischen den Geheimhaltungsinteressen des Verantwortlichen einerseits und dem Recht der betroffenen Person auf klare und umfassende Information andererseits entspricht.

6.9 Datenauswertung freie Mitarbeitende

Im Rahmen meiner Aufsichtszuständigkeit für den Hessischen Rundfunk erreichte mich eine auch formal interessante Anfrage. Es ging um die Prüfung der Zulässigkeit des Vorhabens „Datenauswertung freie Mitarbeitende“, die auf eine entsprechende Anforderung des Gesamtpersonalrates des HR gemäß § 61 Abs. 2 Hessisches Personalvertretungsgesetz (HPVG) zurückgeht: Hat der Personalrat begründete Zweifel an der datenschutzrechtlichen Zulässigkeit eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten der Beschäftigten, kann er eine Stellungnahme der oder des Hessischen Datenschutzbeauftragten fordern.

Nun besteht beim Hessischen Rundfunk die sog. geteilte Zuständigkeit, die auf § 28 Hessisches Datenschutz und Informationsfreiheitsgesetz (HDSIG) zurückgeht, wonach der (Rundfunk)Datenschutzbeauftragte (lediglich) den Datenschutz im journalistischen Bereich zu überwachen hat. Nach meiner Überzeugung tangiert der Einsatz freier Mitarbeitende in der Programmherstellung unmittelbar den journalistischen Bereich, weshalb in Ansehung der geteilten Zuständigkeit nicht die staatliche Aufsicht, sondern der Rundfunkdatenschutzbeauftragte in der Pflicht ist, die Anfrage zu bearbeiten[23].

Die sehr umfangreiche rechtliche Stellungnahme kann hier nicht in allen Einzelheiten wiedergegeben werden, dies würde schlicht den Rahmen eines Tätigkeitsberichtes sprengen. Auf die entscheidenden Rechtsfragen sowie die zugrundeliegenden Erwägungen möchte ich dennoch kurz eingehen.

Der Hessische Rundfunk möchte das Management der freien Mitarbeitenden verbessern und intensivieren. Ziel ist die Auswertung steuerungsrelevanter Daten im Hinblick auf tariflich zugesicherte Auftragsvolumina und Ausfallhonorare. Angestrebt wird die Verbesserung der Informationslage und damit verbesserten Steuerung der freien Mitarbeit durch die Redaktionen. Der Personalrat ist der Auffassung, dass mit der Datenauswertung unzulässige Zwecke verfolgt

[23] Siehe zur Problematik der geteilten Zuständigkeit insbesondere die Kommentierung zu § 28 HDSIG in Rossnagel, Hessisches Datenschutz- und Informationsfreiheitsgesetz 1. Auflage 2021

werden und zumindest der verfolgte Zweck nicht mit demjenigen zu vereinbaren ist, für den die Daten der Mitarbeitenden ursprünglich erfasst worden sind.

Der Hessische Rundfunk wiederum kommt nach Stellungnahme des seinerzeitigen Datenschutzbeauftragten zu dem Ergebnis, dass ein zulässiger Zweck vorliege, der in der Steuerung der freien Mitarbeitenden begründet liege. Die Datenverarbeitung sei zum Erreichen dieses Zwecks erforderlich und auch geeignet, ein milderes Mittel stehe nicht zur Verfügung.

Nach meiner Auffassung ist die in Rede stehende und strittige Datenverarbeitung rechtmäßig gemäß Art. 6 Abs. 1 lit. e DSGVO i.V.m. § 2, § 18 Abs. 1 des Gesetzes über den Hessischen Rundfunk, § 26 Medienstaatsvertrag.

Ich habe im Wesentlichen argumentiert, dass der Hessische Rundfunk einen verfassungsrechtlichen und gesetzlich ausgestalteten Auftrag zu erfüllen hat. Die Rundfunkfreiheit nach Art. 5 Abs. 1 Satz 2 GG wird hiermit konkretisiert. Diese Aufgabe wird wahrgenommen durch die Produktion von Rundfunk und Telemedien und dem damit verbundenen Einsatz von programmgestaltenden (freien) Mitarbeitenden. Die Personalorganisation ist von der Rundfunkfreiheit also mitumfasst und damit auch geschützt. Die Programmfreiheit erlaubt es den Rundfunkanstalten, programmgestaltendes Personal flexibel einzusetzen. Aus dieser Aufgabe folgt wiederum auch das Recht zu einer Verarbeitung personenbezogener Daten, wenn es zur Erfüllung des öffentlich-rechtlichen Auftrages erforderlich ist.

Auf den von mir zu beurteilenden Fall angewendet heißt dies, dass der HR Daten von freien Mitarbeitenden zur Auftragserfüllung in der erforderlichen Weise verarbeiten darf. Nach eingehender Prüfung bin ich unter Berücksichtigung der vorgetragenen Argumente zu dem Ergebnis gekommen, dass der Hessische Rundfunk mit der beschriebenen Datenverarbeitung sowohl im Hinblick auf die Auftragserfüllung als auch zur Einhaltung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit berechtigt ist. Ich hatte zu berücksichtigen, dass die Datenverarbeitung und der damit verbundene zielgenauere Einsatz der Mitarbeitenden dem verfassungsrechtlichen Auftrag im Hinblick auf Wirtschaftlichkeit und effizienten Einsatz der Mittel entspricht, in dem die tarifvertraglichen Ansprüche auf das erforderliche Maß begrenzt werden. Im Ergebnis kann dem HR nicht verwehrt werden, die Kontrolle über die Beschäftigungslage und damit die Minimierung eines Zahlungsrisikos zu behalten.

Ich bin ausdrücklich nicht der Auffassung der Vertreter der Personalräte gefolgt, dass die aus den in diesem Fall einschlägigen Tarifverträgen erwachsenen Rechte der freien Mitarbeitenden im Rahmen der Erforderlichkeitsprüfung nicht berücksichtig worden seien. Es wurde argumentiert, dass die strittige Datenverarbeitung dazu führen würde, dass freie Mitarbeitende weniger Aufträge erhalten

und damit wirtschaftlich schlechter gestellt würden. Hier wird übersehen, dass kein voraussetzungsloser Anspruch auf Teilhabe an den tarifvertraglichen Ansprüchen besteht und diese Voraussetzungen vom HR im Sinne des Auftrages zu steuern sind.

Auch im Hinblick auf die Einhaltung der Datenschutzgrundsätze, die im Wesentlichen in Art. 5 DSGVO niedergelegt sind, konnte ich keine Probleme feststellen, die zu einer Rechtswidrigkeit des geplanten Projekts geführt hätten. Allein das Berechtigungskonzept sowie das Schulungskonzept haben Mängel aufgewiesen, die sich insbesondere in Widersprüchlichkeiten und ungenauen Zuordnungen gezeigt haben. Der HR hat diese Hinweise aufgenommen und Korrekturen zugesagt und umgesetzt.

Im Ergebnis bin ich zu dem Schluss gelangt, dass keine grundlegenden Zweifel an der Rechtmäßigkeit der Datenverarbeitung im Zusammenhang mit dem vom HR initiierten Projekt bestehen.

Insofern konnte diese zeitaufwendige und arbeitsintensive Prüfung im Berichtsjahr abgeschlossen werden.

6.10 Führung des VVT durch interne Datenschutzbeauftragte

Ich wurde um meine rechtliche Einschätzung dazu gebeten, ob es vertretbar oder auch empfehlenswert sei, dass interne Datenschutzbeauftragte die Verantwortung für das Führen des Verzeichnisses von Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DSGVO übernehmen (zu Stellung und Aufgaben des Datenschutzbeauftragten siehe Kapitel 7.1.2).

Ich habe geprüft, ob der Datenschutzbeauftragte in diesem Zusammenhang als Teil der verantwortlichen Stelle angesehen werden kann und ob es ggf. sogar eine Verpflichtung des Datenschutzbeauftragten zum Führen eines VVT gibt.

Zunächst ist festzuhalten, dass der Datenschutzbeauftragte nicht als „verlängerter Arm“ der verantwortlichen Stelle angesehen und ihm demzufolge die Rolle des Verantwortlichen im Sinne der DSGVO nicht zugewiesen werden kann. Auf der anderen Seite gestattet Art. 38 Abs. 6 DSGVO, dass der betriebliche Datenschutzbeauftragte auch andere Aufgaben und Pflichten wahrnehmen kann. Es ist sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenskonflikt führen.

Das Gesetz weist die Pflicht zum Führen eines VVT dem Verantwortlichen zu, sodass vieles dafürspricht, dass dies nicht zu den Aufgaben des Datenschutzbeauftragten gehören kann. Zudem ist zu berücksichtigen, dass der Datenschutzbeauftrage in seiner Kontrollfunktion zu prüfen hat, ob das Verfahrensverzeichnis vollständig und gesetzeskonform geführt wird. Für die Erfüllung der

Überwachungsaufgaben des Datenschutzbeauftragten nach Art. 39 Abs. 1 lit. b DSGVO stellt dieses Verzeichnis ein wichtiges Arbeitsmittel dar. Daher widerspricht es nach meiner Auffassung dem gesetzlichen Leitbild des unabhängigen Datenschutzbeauftragten, diesen mit der Aufgabe der Befüllung und Verwaltung des VVT zu betrauen. Im Ergebnis hätte er sich im Rahmen der Führung des VVT bei dieser Aufgabe selbst zu überwachen. Es gibt aber demgegenüber auch die Auffassung, dass die Führung des VVT im Rahmen der Übertragung von zusätzlichen Aufgaben nach Art. 38 Abs. 6 DSGVO möglich ist und nicht zu Interessenkonflikten führt[24].

Im Ergebnis habe ich davon abgeraten, die alleinige Verantwortung für das Führen des Verfahrensverzeichnisses dem Datenschutzbeauftragten zu übertragen. Indes geboten ist die Einbindung in die Erstellung, Aktualisierung und Überprüfung des Verzeichnisses; dies ergibt sich überdies auch aus der gesetzlichen Aufgabenzuweisung.

6.11 Altersfreigabe in der ARD- und ZDF-Mediathek

Immer wieder erreichen mich Anfragen zur ARD- und ZDF-Mediathek, und zwar im Hinblick auf die Datenverarbeitung im Rahmen der Altersbestätigung zur Aufhebung der Altersspерre. Es geht zumeist um die Angabe von Personalausweisdaten bzw. die jugendschutzbezogene Freischaltung des Nachtprogramms auch am Tag, eine missverständliche Formulierung bei der Passworteingabe sowie um ein mögliches Umgehen der Jugendschutz-Sperre.

Hintergrund der Altersfreigabe ist, dass aus Gründen des Jugendschutzes Inhalte, die ab 16 oder 18 Jahren freigegeben sind, erst ab 22:00 Uhr oder 23:00 Uhr ohne Beschränkung in der ARD- oder ZDF-Mediathek bereitgestellt werden dürfen. Wenn also der Wunsch besteht, Sendungen mit Altersbeschränkungen vor den genannten Zeiten anzuschauen, ist es notwendig eine Altersfreigabe einzurichten. Dieses Vorgehen für das frei verfügbare Angebot der Mediathek ist freiwillig.

Das Verfahren des Altersnachweises für die Bestätigung des Alters anhand der Eingabe der Zeichenkombination in der sogenannten maschinenlesbaren Zone der Ausweisdokumente ist ein gängiges und anerkanntes Verfahren.

Im Rahmen der Altersfreigabe wird das Alter einmalig geprüft, dazu ist die Eingabe von Ausweisdaten erforderlich. Es wird nun von Nutzenden teilweise angenommen, dass konkrete Ausweisdaten beim Verantwortlichen gespeichert oder gar Nutzerprofile erstellt werden, dem ist aber nicht so. Die anzugebende Zeichenkombination findet über einen Algorithmus allein dazu Verwendung, das Alter zu bestimmen und zu bestätigen. Nur diese Bestätigung wird vorgehalten, nicht die eingegebenen Daten.

[24] Taeger/Gabel/Scheja DS-GVO Art. 38 Rn. 76

Bemängelt wurde auch ein mögliches Umgehen dieser Jugendschutzsperre mit anderweitiger Software, so dass auch nicht jugendfreie Inhalte ohne Beschränkung konsumiert werden könnten. Eine Beurteilung der Frage, inwieweit damit der Jugendschutz wirksam umgesetzt wird, entzieht sich jedoch meiner Zuständigkeit.

Bei der Einrichtung der Jugendschutz-PIN führte eine missverständlich formulierte Anweisung bei der Eingabe des bestätigenden Passwortes zu Irritationen. Die Anmeldung bei der Mediathek erfolgt mit einem Benutzernamen (E-Mail-Adresse des Nutzenden) und einem spezifisch für die Mediathek gewählten Passwort. Die gesetzte Jugendschutz-PIN soll nun mit eben diesem spezifischen Passwort bestätigt werden. Die entsprechende Anweisung lautete: „Bitte bestätigen Sie den Code mit Ihrem Passwort für <E-Mail-Adresse>“, so dass man auf den Gedanken kommen konnte, dass unberechtigterweise das Passwort für das E-Mail-Postfach beim Provider erfragt würde. Durch eine Umformulierung dieser Anweisung konnte der Beschwerde abgeholfen und Eindeutigkeit hergestellt werden.

6.12 Rechnungshöfe und Datenschutz

Sind die verantwortlichen Landesrundfunkanstalten befugt, den Rechnungshöfen personenbezogene Daten im Zuge von Prüfungen zu übermitteln? Im Berichtsjahr hat mich diese Frage vom SWR erreicht, sie ist aber nach meiner Einschätzung auf sämtliche Rundfunkanstalten zu übertragen.

Die Prüfungsrechte der Landesrechnungshöfe sind unbestritten, die Vorschriften der Landeshaushaltsordnungen sind entsprechend anzuwenden. Die Prüfung beschränkt sich regelmäßig darauf, ob die Haushalts- und Wirtschaftsführung der Rundfunkanstalt wirtschaftlich und sparsam erfolgt ist. Dem prüfenden Rechnungshof sind diejenigen Unterlagen zu übersenden, die er zur Erfüllung seiner Aufgaben für erforderlich hält. Im Rahmen der Beurteilung der Erforderlichkeit kommt es also maßgeblich auf die Einschätzung des Rechnungshofes an, ihm kommt weiter Ermessungsspielraum zu.

Genau zu prüfen ist in dem Zusammenhang, was bei der Anforderung personenbezogener Daten durch die Rechnungshöfe gilt.

Nach Vorschriften der Landesdatenschutzgesetze (im vorliegenden Fall § 4 LDSG-BW) ist eine Verarbeitung von personenbezogenen Daten dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit einer öffentlichen Stelle liegenden Aufgabe erforderlich ist. Die Verarbeitung der im Rahmen der Prüfung angeforderten personenbezogenen Daten muss demzufolge für die Erfüllung der Aufgaben des Rechnungshofes erforderlich sein.

Ich bin der Auffassung, dass es einer expliziten Vorschrift nicht bedarf, die die Rechnungshöfe dazu ermächtigt, personenbezogene Daten zu erheben und im Rahmen ihrer Prüfung zu verarbeiten. Es ist davon auszugehen, dass § 4 LDSG-BW i.V.m. den Vorschriften des SWR-Staatsvertrages und der Landeshaushaltsordnung eine geeignete Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten durch den Rechnungshof im Rahmen dessen Prüfung darstellt.

Zu beachten ist allerdings, dass die Prüfung die Programm- und Finanzautonomie der öffentlich-rechtlichen Rundfunkanstalten, hier des SWR, wahren muss und nicht in unzulässiger Weise in die Rundfunkfreiheit eingegriffen werden darf. Nur wenn diese Grenzen im Rahmen einer Abfrage beachtet werden, kann auch eine Herausgabe von personenbezogenen Daten datenschutzrechtlich in Frage kommen. Als Beispiele können der Vollzugriff auf die Personalakten der freien Mitarbeitenden des SWR oder Fragen zur Finanzierung von Produktionen genannt werden. Ebenso gilt zweifellos, dass die Rechnungshöfe die Vorgaben der DSGVO einzuhalten haben. Insbesondere die Grundsätze des Art. 5 DSGVO finden Anwendung und dort wiederum ist die Datenminimierung zu beachten. Die personenbezogenen Daten, die der Rechnungshof im Rahmen seiner Prüfung verarbeiten möchte, müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Hier sind also den Forderungen der Rechnungshöfe Grenzen gesetzt, wenn bei sehr umfassenden Datenzugriffen eine Erforderlichkeit und damit auch die Verhältnismäßigkeit in Zweifel gezogen werden kann.

Aus meiner Sicht sind daher die Rechnungshöfe gehalten, sehr genau zu prüfen und auch darzulegen, warum die Daten für die Prüfung erheblich sind und sie auf das notwendige Maß zu beschränken. In den Blick zu nehmen ist, ob der Verarbeitungszweck (hier die konkrete Rechnungshofprüfung mit der Zielrichtung Wirtschaftlichkeit und Sparsamkeit) auch mit weniger oder keinen personenbezogenen Daten erreicht werden kann. Indes ist nicht pauschal ausgeschlossen, dass die Rechnungshöfe personenbezogene Daten für ihre Prüfungen benötigen. Eine Einzelfallprüfung wird stets unumgänglich sein, die verantwortlichen Rundfunkanstalten sind aufgefordert, den Rechnungshöfen gegenüber die Einhaltung des Datenschutzrechtes anzumahnen.

6.13 Nutzung von WhatsApp im Rahmen der Zuschauerkommunikation

Gelegentlich erreichen mich Zuschriften, die mit teils harschen Worten die Nutzung von WhatsApp als Kanal für Zuschauerreaktionen kritisieren. Der Schutz der personenbezogenen Daten der Nutzenden wird häufig als wenig vertrauenswürdig erachtet, ebenso aber die Tatsache bemängelt, dass damit die Marktvormacht dieses Messengers befördert und quasi „Schleichwerbung“ betrieben werde.

Obwohl nur am Rande Datenschutzthemen adressiert werden, fühle ich mich dennoch aufgerufen, zu solcherlei Vorwürfen Stellung zu nehmen. Neben der Tatsache, dass die grundsätzlich

ablehnende Haltung zu WhatsApp nachvollziehbar scheint, mache ich darauf aufmerksam, dass es dem öffentlich-rechtlichen Rundfunk auch freistehe, über diesen Kanal Nutzerinnen und Nutzer zu erreichen. Ich verweise auf § 30 Abs. 4 Satz 5 Medienstaatsvertrag (MStV) wonach der öffentlich-rechtliche Rundfunk und damit auch die einzelnen Rundfunkanstalten, Telemedien außerhalb der jeweils eigenen Portale anbieten können. Es ist auch Aufgabe des öffentlich-rechtlichen Rundfunks in einem dynamischen Medien- und Meinungsmarkt ein die Vielfalt sicherndes Gegengewicht zu bilden. Es ist unbestreitbar, dass auf Social Media Plattformen ein Großteil der Meinungsbildung stattfindet, weshalb Nutzerinnen und Nutzer von den öffentlich-rechtlichen Rundfunkanstalten auch auf diesen Netzwerken angesprochen werden sollen. Diese besondere Aufgabe des öffentlich-rechtlichen Rundfunks berechtigt nach meiner Auffassung dazu, auch andere Ausspielwege als die eigenen Plattformen zu wählen. Wichtig ist aus meiner Sicht immer, dass nicht ausschließlich über diese Kanäle kommuniziert wird, sodass es den Nutzerinnen und Nutzern freisteht, datenschutzrechtlich unbedenkliche Kanäle wie die eigenen Plattformen der Rundfunkanstalten zu nutzen. Ebenso muss in den Datenschutzerklärungen über Social Media und die Einbindung von Messengern ausführlich unterrichtet werden, und es sollten auch datenschutzfreundliche Alternativen wie bspw. Signal oder Threema angeboten werden.

Es steht also in der Verantwortung der Rundfunkanstalten, sich dieses Themas immer wieder bewusst zu werden und gleichsam datenschutzrechtlich unbedenkliche Angebote zu machen.

6.14 Gewinnspiel

Im Berichtsjahr erreichte mich eine Beschwerde bezüglich der Teilnahme- und Datenschutzbedingungen zu dem von WDR 4 veranstalteten Gewinnspiel „Weihnachtsbonus mit Edeka“. Bemängelt wurden

- der zu allgemein gefasste Zeitpunkt der täglichen Gewinnspielrunde,
- nicht eindeutig formulierte Teilnahmebedingungen im Hinblick auf die Kandidaten- und Gewinnerauswahl sowie die Gewinnverkündung,
- eine unzureichende Information zur Datenverarbeitung im Gewinnfall und zur Datenweitergabe an „angeschlossene Partner“.

Eine Prüfung ergab, dass die bemängelten Punkte zwar grundsätzlich durchdacht waren, dass diese jedoch nicht ausreichend transparent den Weg an die Öffentlichkeit gefunden hatten. Außerdem wurde keine nachweisbare Einwilligung für die Datenverarbeitung zur Teilnahme eingeholt. Da das Gewinnspiel zwischenzeitlich ausgelaufen war, konnte eine Korrektur der Teilnahme- und Datenschutzbedingungen allerdings nicht mehr vorgenommen werden.

Für eine nachhaltige Optimierung von Gewinnspielprozessen des WDR wurde jedoch zugesichert, dass in Ansehung der berechtigten Beschwerdepunkte ein Dokument erstellt und den relevanten

Stellen des WDR zur Verfügung gestellt wird, das die Grundlagen für eine rechtssichere Gewinnspielveranstaltung und Formulierung der Teilnahmebedingungen zusammenfasst.

7 Datenschutz in den Rundfunkanstalten

Dieses Kapitel soll einen Überblick geben über die grundsätzliche Datenschutzorganisation in den von mir beaufsichtigten Anstalten und Schwerpunkte skizzieren. Daher beschränke ich mich an dieser Stelle insbesondere auf die Erkenntnisse, die ich gemeinsam mit meinem Team in den vierteljährlich stattfindenden Jour fixes mit den internen Datenschutzbeauftragten der Rundfunkanstalten gewonnen habe. Über einzelne Themen, die mich im Zusammenhang mit Beratungen oder auch auf sonstigen Wegen aus den Rundfunkanstalten erreicht haben, berichte ich in Kapitel 6. Davon unabhängig gehört es zu meinen Aufgaben, Schulungen durchzuführen oder auch für telefonische Beratungen zur Verfügung zu stehen. Im Berichtsjahr habe ich bspw. einen Vortrag zu KI und Datenschutz auf der Personalleitertagung von ARD, ZDF und Deutschlandradio gehalten. Auf eine ausführliche Berichterstattung dazu wird aus Kapazitätsgründen verzichtet.

Dies vorausgeschickt beziehen sich die nun folgenden Berichtspunkte auf die Gespräche und den Austausch mit den internen Datenschutzbeauftragten. Die Durchführung von Jour fixes erweist sich nach meiner Überzeugung als taugliches Instrument, um die Gegebenheiten unter dem Blickwinkel des Datenschutzes in den einzelnen Rundfunkanstalten vergleichen und wichtige Erkenntnisse über die Schwerpunktsetzung sowie über die Entwicklungen der Datenschutzorganisation in den Rundfunkanstalten gewinnen zu können.

7.1 Quartalsweiser Austausch mit den Rundfunkanstalten

Als Aufsichtsbehörde für Datenschutz gebietet sich eine gewisse Distanz zum Tagesgeschäft der Rundfunkanstalten. Einerseits berate ich als Rundfunkdatenschutzbeauftragter zu Anfragen, dies findet in unregelmäßigen Abständen statt. Um meinen aufsichtsrechtlichen Blick zu schärfen und einen Einblick in die Fragen und Themen, Herausforderungen, Bedürfnisse rund um den Datenschutz in den Rundfunkanstalten zu erhalten, habe ich andererseits im Jahr 2024 einen vierteljährlichen Jour fixe mit den jeweiligen Datenschutzbeauftragten (und optional deren Stellvertretungen oder direkten Assistenzen) ins Leben gerufen. Dazu habe ich auch die Datenschutzbeauftragte des Beitragsservices eingeladen, da mich als ein Schwerpunkt meiner Aufgaben Datenschutzthemen im Rahmen des Beitragseinzuges beschäftigen. Insgesamt haben mein Team und ich so in jedem Quartal zehn Jour Fixes durchgeführt und ausgewertet. Der Fragen- und Themenkatalog hat sich dabei weiterentwickelt und geschärft.

Insgesamt haben die Jour fixes sich als ein wirksames Instrument erwiesen, um mir einen Überblick darüber zu verschaffen, wie Datenschutz in den Rundfunkanstalten organisiert ist und gelebt wird. Durch die wiederkehrende Fokussierung auf bestimmte Themen war es möglich, Entwicklungen zu beobachten, diese zu bewerten und potenzielle Maßnahmen für meine Aufsichtstätigkeit abzuleiten.

7.1.1 Organisation des Datenschutzes

Datenschutz wird in allen Rundfunkanstalten beachtet und gelebt, ist dort aber abhängig von der Größe und Struktur der Rundfunkanstalten unterschiedlich organisiert. Während einige Rundfunkanstalten mehr Ressourcen für den Datenschutz vorhalten, fällt auf, dass in manchen Rundfunkanstalten vergleichsweise geringe Datenschutz-Kapazitäten zur Verfügung stehen. Im Hinblick auf die in Art. 39 DSGVO definierten Aufgaben von Datenschutzbeauftragten sollten diese allerdings mit ausreichend Zeit und Mitteln ausgestattet sein – das betrifft sowohl die Kapazitäten der Datenschutzbeauftragten selbst als auch ergänzende Ressourcen von Datenschutz-Schnittstellen in den Fachabteilungen der Rundfunkanstalt (z.B. Datenschutzkoordinatoren).

Aus den Jour fixes mit den Datenschutzbeauftragten der Rundfunkanstalten im Berichtsjahr lässt sich ableiten, dass Dreh- und Angelpunkte für funktionierende Datenschutzprozesse sowohl ausreichende Ressourcen als auch eine Prozessdokumentationen und aktive Mitarbeit der Datenschutzkoordinatoren und Mitarbeitenden in den Fachbereichen sind. Ein aktives Engagement beim Entwickeln der Datenschutzprozesse durch die Datenschutzkoordinatoren könnte teilweise noch ausgebaut werden. Es wird den Rundfunkanstalten empfohlen, dies nachdrücklich einzufordern. Die vorhandenen Datenschutz-Ressourcen sollten in einem angemessenen Verhältnis zu den anstehenden Aufgaben/Projekten stehen und kontinuierlich überprüft und angepasst werden.

7.1.2 Stellung und Aufgaben der internen Datenschutzbeauftragten

Art. 39 DSGVO bestimmt die Aufgaben des internen Datenschutzbeauftragten. Dazu gehören u.a. die Unterrichtung und Beratung des Verantwortlichen hinsichtlich der Pflichten nach der DSGVO sowie auch Überwachung der Einhaltung der DSGVO. Letztendlich bedeutet das die Überprüfung der Einhaltung von datenschutzrechtlichen Vorschriften bei den Verarbeitungsverfahren, und ob und inwieweit durch interne Vorgaben und Richtlinien die Einhaltung der datenschutzrechtlichen Bestimmungen ausreichend sichergestellt wird. Eine eigene Entscheidungskompetenz – dies ist ganz wichtig – kommt ihm insgesamt nicht zu[25]; die Rolle erschöpft sich in ihrer beratenden und

[25] Vgl. dazu ausführlich Beck OK Datenschutzrecht DSGVO Art. 39 Rn. 8 ff.

überwachenden Funktion. Wichtig ist überdies die Unabhängigkeit der internen Datenschutzbeauftragten, d.h. jegliche Einflussnahme ist verboten. Sie dürfen keine Anweisungen bei der Erfüllung ihrer Aufgaben erhalten (Art. 38 Abs. 3, S. 1 DSGVO).

In der Praxis erweist sich die Umsetzung und genaue Auslegung dieser Vorschriften als nicht immer einfach, denn es besteht die natürliche Neigung, den oder die Datenschutzbeauftragte als „Sachbearbeiter“ in Datenschutzfragen einzusetzen, was nicht der Rolle nach der DSGVO entspricht. Insofern stellt sich die Frage, in welchem Maß die oder der Datenschutzbeauftragte in die operative Steuerung des Datenschutzes in den Rundfunkanstalten eingreifen kann.

Im Rahmen der regelmäßigen Gespräche in den Jour fixes hat sich gezeigt, dass diejenigen Datenschutzbeauftragten, die aktiv, unterstützend und initiativ an der Umsetzung von datenschutzrechtlichen Vorgaben mitwirken, effektiver und damit auch erfolgreicher wirken können. Dies halte ich aus pragmatischen Erwägungen auch für völlig in Ordnung und würde es sogar unterstützen. Wichtig ist allerdings, dass sowohl der Datenschutzbeauftragte als auch die verantwortliche Stelle sich stets bewusst sind, dass die Grenze der Unabhängigkeit und Weisungsfreiheit nicht überschritten werden darf. Ebenso muss darauf geachtet werden, dass der Datenschutzbeauftragte nicht „quasi von selbst“ an die Stelle des Verantwortlichen rückt, der die anstehenden (Datenschutz-)Aufgaben an den engagiert und aktiv arbeitenden Datenschutzbeauftragten abgibt. Insofern gilt es hier stets aufmerksam zu bleiben und die Rollenverteilung immer wieder zu hinterfragen. Aus meiner Sicht sind die internen Datenschutzbeauftragten aber auch aufgerufen, ihre Rolle aktiv und entsprechend ihrer Aufgabenzuweisung umfassend zu erfüllen. Dies spielt insbesondere dort eine Rolle, wo ein Datenschutzmanagementsystem (DSMS) noch nicht oder noch nicht vollständig etabliert ist. Der oder die Datenschutzbeauftragte kann aktiv an der Erarbeitung eines solchen Systems mitwirken, da ein solches gleichsam die Voraussetzung für eine wirksame Überprüfung der Prozesse darstellt. Durch sein Zutun bei der Entwicklung kann er damit auch die Rechtmäßigkeit und Vollständigkeit eines solchen Systems überwachen, so wie es die DSGVO vorsieht.

Erneut wird betont: Um diese Rolle ausführen zu können, bedarf es einer oder eines strukturell gut aufgestellten Datenschutzbeauftragten. Ihr oder ihm müssen ausreichend zeitliche Ressourcen zur Verfügung stehen sowie die Arbeitsmittel, die es zur Erfüllung ihrer oder seiner Aufgaben braucht. Die Verantwortlichen sind aufgerufen, sensibel auf entsprechende Anforderungen zu reagieren und diese nicht mit Blick auf (gewiss erforderliche) Sparbemühungen gleichsam im Keim zu ersticken.

7.1.3 Berichtsweg an das Management

Der Bericht zu Datenschutztätigkeiten an das Management (vgl. Art. 38 Abs. 3, S. 3 DSGVO) fällt in den einzelnen Rundfunkanstalten sehr unterschiedlich aus. In einigen erstellen die Datenschutzbeauftragten einen jährlichen Datenschutzbericht oder fertigen Aktenvermerke für die Geschäftsleitung; teilweise wird der Datenschutzbericht in der Direktorensitzung vorgestellt. Anstelle eines Datenschutzberichtes finden in manchen Rundfunkanstalten regelmäßige oder bedarfsorientierte Jour fixes mit Vertretern der Geschäftsführung statt.

Es ist zu begrüßen, dass in allen Rundfunkanstalten an das Management berichtet wird. Ziel dabei sollte stets das Hinwirken auf einen aktiven Austausch und eine Bewertung von offenen Themen/Empfehlungen sein, um diese ggf. in zielführende Maßnahmen zu übersetzen.

7.1.4 Einführung bzw. Weiterentwicklung eines Datenschutz-Managementsystems

Nach Art. 5 Abs. 2 DSGVO müssen Verantwortliche die Grundsätze für die Verarbeitung personenbezogener Daten einhalten und nachweisen können. Um eine solche Nachweisführung in einem ähnlich strukturierten Format zu fördern, hat der Arbeitskreis der Datenschutzbeauftragten (AK DSB) eine Vorlage für die Dokumentation eines Datenschutz-Managementsystems (DSMS) und der damit einhergehenden Prozesse und Verantwortlichkeiten für Planung, Organisation, Steuerung und Kontrolle der gesetzlichen und betrieblichen Anforderungen an den Datenschutz erstellt und im 4. Quartal 2023 veröffentlicht (siehe hierzu auch Kapitel 8.2 meines letztjährigen Berichts). Diese kann als Basis für die Dokumentation eines DSMS genutzt werden.

Einer der Kernpunkte der Jour fixes war der Austausch zum Stand der Einführung bzw. Weiterentwicklung eines DSMS und die Verdeutlichung der Notwendigkeit eines strukturierten und umfassend dokumentierten Datenschutzmanagements. Im Hinblick auf den jeweiligen Arbeitsstand in den Rundfunkanstalten lässt sich zusammenfassen, dass grundsätzlich alle die Umsetzung vorantreiben, es hinsichtlich des erreichten Standes noch Unterschiede gibt: Während sich bei einigen ein DSMS und ein kontinuierlicher Verbesserungsprozess etabliert haben, befinden sich andere noch mitten in der Bündelung und Revision bestehender Dokumentationen, auf dem Weg zu einem DSMS oder sind erst in der Projektplanung.

Ziel für die durch mich beaufsichtigten Rundfunkanstalten sollte es sein, dass diese im Jahr 2025 ihr DSMS intern veröffentlichen, um es anschließend in einen Prozess der kontinuierlichen Verbesserung zu überführen. Den Stand der Bemühungen werde ich in den Jour fixes im Jahr 2025 weiter beobachten und - wo immer notwendig - unterstützen.

7.1.5 Beschwerden und Auskunftsanfragen

Thema der Jour fixes war auch die Anzahl eingegangener Beschwerden und Auskunftsanfragen, und zwar mit dem Fokus auf den Prozess einer kontinuierlichen Verbesserung der abgeleiteten Maßnahmen.

Das Management der Eingaben von Betroffenen wird in den Rundfunkanstalten unterschiedlich gehandhabt. Während teilweise alle Datenschutz-Eingaben über den Tisch des Datenschutzbeauftragten gehen, steuern und filtern andere Rundfunkanstalten im Vorfeld bereits die Anfragen und weisen diese bestimmten Stellen zu. In Abhängigkeit von Größe und Sendegebiet der Rundfunkanstalten kann dies eine praktikable Lösung sein, um Datenschutzbeauftragte bereits im Vorfeld von der richtigen Zuweisung der Eingabe innerhalb des Hauses zu entlasten.

Meiner Kenntnis nach ging in den Rundfunkanstalten über die Quartale hinweg eine überschaubare Anzahl an nicht den Beitragsservice betreffenden Auskunftsanfragen und Datenschutzbeschwerden ein. Dagegen mehrten sich im Verlauf des Jahres eingehende Standardschreiben, mit denen dem Rundfunkbeitragseinzug widersprochen wurde. Diese waren auf die kostenpflichtigen Plattform-Dienste von www.beitragsblocker.de und www.beitragsstopper.de zurückzuführen (siehe hierzu ausführlich Kapitel 8.3).

7.1.6 Kontinuierliche Themenschwerpunkte in den Rundfunkanstalten

Über alle Rundfunkanstalten hinweg gab es Themen und konkrete Verarbeitungsvorgänge, mit denen sich diese im Hinblick auf Datenschutz und Datensicherheit kontinuierlich und tiefergehend beschäftigten.

So wurden für Softwarebeschaffungen gemeinsame Lösungen angestrebt und datenschutzrechtlich bewertet. Daneben wurden uns Themen aus den Redaktionen, der Verwaltung sowie IT-sicherheitsspezifische Sachverhalte mit datenschutzrechtlichen Anknüpfungspunkten vorgestellt.

Ich habe den Eindruck gewonnen, dass dieser kontinuierliche und themenbezogene Austausch gut geeignet ist, eng an die „Datenschutzrealität“ der Rundfunkanstalten anzuknüpfen. Wie bereits eingangs geschildert, bereiten wir diese Termine intensiv vor und lassen den Rundfunkanstalten im Vorfeld Fragen zukommen, die besprochen werden. Stets werden die Punkte, die in dem Jour fixe zuvor diskutiert wurden, wieder aufgegriffen. So kann sich über das Jahr hinweg ein anschauliches Bild ergeben, das mir gute Eindrücke des gelebten Datenschutzes in den Rundfunkanstalten vermittelt. Ich werde diese Praxis auch im Jahr 2025 fortführen.

7.2 Überprüfung der Datenschutzhinweise auf Homepages der Rundfunkanstalten

Am Anfang des Jahres 2024 haben wir die Datenschutzhinweise auf den Websites der Rundfunkanstalten und ausgewählter Beteiligungsunternehmen in den Blick genommen. Der Fokus lag hier zunächst auf einem korrekten Hinweis auf die Aufsichtsbehörde sowie einer leicht auffindbaren Veröffentlichung der Tätigkeitsberichte.

Festzustellen war, dass bei den meisten Rundfunkanstalten mein seinerzeit aktueller Tätigkeitsbericht bereits veröffentlicht war oder darauf verwiesen wurde. Diejenigen, bei denen dies nicht der Fall war, haben nachgebessert. Kontaktdaten des Rundfunkdatenschutzbeauftragten waren durchgehend vermerkt, leider teilweise auf einem veralteten Stand, so dass wir, wo nötig, um Korrektur gebeten und die Nutzung eines von uns vorgegebenen einheitlichen Adressblockes empfohlen haben. Die Anpassungen veralteter Daten wurden umgesetzt, ebenso wurde auf den meisten Seiten der empfohlene Aufsichtsadressblock platziert.

Wenn in den Seiten zum Datenschutz vermerkt ist, wann die letzte Änderung vorgenommen wurde („Stand“), scheint dies eine Ermunterung zu sein, sich um Aktualisierungen zu kümmern. Zumindest hat unsere Erhebung gezeigt, dass Datenschutzseiten mit Datum der letzten Anpassung aktueller und akkurater waren. Davon ausgehend empfehle ich, den Stand der letzten Anpassung in der Datenschutzerklärungen zu ergänzen.

Grundsätzlich ist zu empfehlen, Datenschutzthemen ebenso prozessbezogen zu betrachten und Änderungsnotwendigkeiten auf alle betriebenen Websites zu übertragen; hierfür ist es sinnvoll einen Prozessverantwortlichen zu benennen, dem die Steuerung obliegt. Ich erwäge eine Untersuchung rund um die Prozesse zur Erstellung und Implementierung von Datenschutzhinweisen in allen Medien (Websites, Apps, Newsletter usw.) aufzusetzen und diese sowohl bei den Rundfunkanstalten als auch den Beteiligungsunternehmen durchzuführen.

8 Datenschutz beim Beitragsservice

8.1 Kostenpflichtiger Online-Service für Rundfunkbeitragsangelegenheiten

Durch den Beitragsservice bin ich auf die Seite www.service-rundfunkbeitrag.de[26] aufmerksam gemacht worden, auf der kostenpflichtige Dienstleistungen zum Rundfunkbeitrag angeboten wurden. U.a. gab es dort Online-Formulare zur Abmeldung einer Wohnung, zur Änderung des Beitragskontos, zur Erstanmeldung einer Wohnung oder auch zur Anmeldung einer weiteren Wohnung.

Auf der Seite www.rundfunkbeitrag.de – also der offiziellen Seite des Beitragsservice von ARD, ZDF und Deutschlandradio – gibt es ebenfalls Formulare, mit denen man solche Änderungen zum Beitragskonto mitteilen kann, jedoch selbstverständlich ohne zusätzliche Kosten. Seitens des Beitragsservice wurde ich gebeten zu prüfen, ob ich als Aufsichtsbehörde Möglichkeiten sehe, dem Vorgehen des kommerziellen Anbieters Einhalt zu gebieten.

Nach Sichtung des Angebots erschien dieses schon deshalb unzulässig oder zumindest fragwürdig, weil nach meiner Ansicht intransparent geblieben ist, was mit den Daten der Nutzerinnen und Nutzern geschieht. Die auf der Website auffindbare Datenschutzerklärung schien wenig aussagekräftig.

Dennoch konnte ich an dieser Stelle im Rahmen meiner Aufsichtszuständigkeit nicht weiterhelfen, denn bei diesem Online-Angebot bin ich nicht die richtige Datenschutzaufsichtsbehörde. Laut Impressum befand sich das Unternehmen in Rheinland-Pfalz, sodass der dortige Landesdatenschutzbeauftragte ggf. Sanktionen im Hinblick auf Datenschutzverstöße verhängen kann.

Zwischenzeitlich hatten sich auch die Verbraucherzentralen (Verbraucherzentrale Sachsen-Anhalt und Verbraucherzentrale Bundesverband) der Sache angenommen und Abmahnungen ausgesprochen. Ebenso ist eine Sammelklage eingereicht worden. Hintergrund war, dass das Unternehmen eine Gebühr für die Nutzung eines Online-Formulars zum Rundfunkbeitrag verlangte, ohne auf die Kosten deutlich hinzuweisen.

[26] Diese Website ist mittlerweile nicht mehr erreichbar, jedoch werden diese Angebote nun auf www.dein-rundfunkbeitrag.de verfügbar gemacht. Das Impressum wurde erneuert und dort wird an erster Stelle mit einer Einblendung darüber informiert, dass es sich um einen unabhängigen Onlineservice handelt und auf die Services des Beitragsservice von ARD, ZDF und Deutschlandradio verlinkt.

Das auf den ersten Blick seltsame Ergebnis, dass im Rahmen dieses „Services“ zwar die Beitragsnummer verarbeitet wurde, dies jedoch mit dem Beitragsservice nichts zu tun hat, erklärte sich allein dadurch, dass die Nutzerinnen und Nutzer im Rahmen dieser – aus meiner Sicht fragwürdigen – Serviceleistung ihre Daten freiwillig angegeben hatten. Insgesamt war dies ein auch aus Datenschutzsicht sehr misslicher Umstand, da dies den Ruf des öffentlich-rechtlichen Rundfunks in Deutschland beschädigen könnte. Dennoch war mir aus aufsichtsrechtlicher Sicht keine Handhabe gegeben.

8.2 Beschwerdevorlagen gegen die Datenverarbeitung beim Beitragsservice und die Datenweitergabe an Vollstreckungsbehörden

Mich erreichten im Berichtsjahr insgesamt 46 Eingaben mit gleichlautendem Inhalt, überschrieben mit „Anzeige Verstoß gegen die Datenschutzgrundverordnung“ sowie „Datenherausgabe“.

In den meisten Fällen werden die Beschwerden gegenüber den staatlichen Datenschutzaufsichtsbehörden erhoben, die diese dann zuständigkeitshalber an meine Behörde weiterleiten.

Die Beschwerden, deren Herkunft Internetseiten zuzurechnen ist, die zum Teil kostenpflichtig Formulierungsvorlagen zur Verfügung stellen, um mit fadenscheinigen Argumenten gegen die Rechtmäßigkeit der Einziehung der Rundfunkbeiträge Stimmung zu machen, werden von mir in der Weise beantwortet, dass ich auf die zentralen Vorwürfe der Schreiben unter Nennung der Rechtsgrundlagen eingehe.

Zentrale Vorwürfe der Schreiben sind das Nichtvorliegen eines Einverständnisses zur Weitergabe der personenbezogenen Daten der betroffenen Beitragszahler vom Einwohnermeldeamt an den als „Dritte“ bezeichneten Beitragsservice, sowie die Weitergabe der personenbezogenen Daten des Beitragsservice an staatliche Vollstreckungsstellen.

Die Übermittlung von Daten der Einwohnermeldeämter an den Beitragsservice ist entgegen der Auffassung der Beschwerdeführer allerdings gesetzlich geregelt. Rechtliche Grundlage ist § 11 Rundfunkbeitragsstaatsvertrag (RBStV) und dort die Absätze 4 und 5.

Weiter wird in dieser Musterbeschwerde der Gesetzesrang des Rundfunkbeitragsstaatsvertrags verneint. Das weise ich in meinen Antworten deutlich zurück und erläutere, dass der Staatsvertrag als Gesetz anzusehen ist, da es sich dabei um einen Vertrag zwischen den Bundesländern handelt, dem die Ministerpräsidenten aller 16 Landesparlamente zugestimmt haben. Insofern kommt es auf

die Gesetzgebungskompetenz des Bundes nicht an und ebenso wenig handelt es sich dabei um einen öffentlich-rechtlichen Vertrag, auf den die Beschwerden mit Nennung des § 58 VwVfG (Verwaltungsverfahrensgesetz) Bezug nehmen.

Zur Weitergabe der personenbezogenen Daten des Beitragsservice an die staatliche Vollstreckungsstelle, weise ich auf § 10 Abs. 6 RBStV hin, wonach der Beitragsservice befugt ist, Festsetzungsbescheide im Verwaltungsvollstreckungsverfahren durch die zuständige Vollstreckungsbehörde durchsetzen zu lassen; dies setzt notwendigerweise die Übermittlung der entsprechenden personenbezogenen Daten an diese voraus.

Ich mache darüber hinaus in meiner Antwort klar, dass die mit der Abwicklung eines Beitragsverhältnisses verbundene Datenverarbeitung einschließlich der Weitergabe personenbezogener Daten an die zuständige Vollstreckungsbehörde lediglich die notwendige Folge eines tatsächlichen oder vermeintlichen Verstoßes gegen die Beitragspflicht ist.

Anhand dieses Beispiels zeigt sich einmal mehr, dass Beitrags- und Datenschutzrecht voneinander zu trennen und abzugrenzen sind: Bevor die beitragsrechtlichen Streitigkeiten nicht geklärt sind, kann die Frage nach der damit verbundenen Rechtmäßigkeit der Datenverarbeitung nicht abschließend beantwortet werden.

8.3 Unterlassungsaufforderungen - Anfragen von Meldebehörden

Zum Ende des Berichtsjahres erreichten mich auch vermehrt Beratungsanfragen von Stadt- und Gemeindeverwaltungen.

Die Meldebehörden werden jeweils mit einem umfangreichen Mustertext von Bürgern angeschrieben, der mit „Unterlassungsaufforderung Anforderung einer Datenauskunft nach Art. 15 DSGVO sowie Widerspruch nach Art. 22 DSGVO“ überschrieben ist und deren Herkunft Widerspruchsvorlagen im Internet (www.beitragssstopper.de, www.beitragsblocker.de) sind, die die Erhebung der Rundfunkbeiträge grundsätzlich als rechtswidrig erachten.

Bei der in diesen Schreiben aufgeworfenen Rechtsfrage geht es vor allem darum, ob die Städte und Gemeinden berechtigt sind, Meldedaten an den Beitragsservice von ARD, ZDF und Deutschlandradio zu übermitteln. Es wird seitens der Beschwerdeführer argumentiert, dass der Beitragsservice nicht rechtsfähig sei und daher die Übermittlung an ihn durch § 34 Abs. 1 BMG nicht gerechtfertigt werden könne.

Auch wenn die Übermittlung der Meldedaten durch die Meldebehörden staatliches Verwaltungshandeln betrifft und daher grundsätzlich keine Zuständigkeit des Rundfunkdatenschutzbeauftragten gegeben ist, berate ich die Gemeinden aufgrund der Sachnähe kurz zu den Rechtsgrundlagen aus dem Rundfunkbeitragsstaatsvertrag.

Ich weise aufgrund des in den Beschwerden enthaltenen Vorwurfs eines Datenschutzverstoßes mit der Begründung, der Beitragsservice sei nicht rechtsfähig, darauf hin, dass bei der Beauftragung des Beitragsservice als gemeinsame Stelle aller Rundfunkanstalten nach § 10 Abs. 7 Rundfunkbeitragsstaatsvertrag (RBStV) gemäß § 11 Abs. 2 RBStV immer eine Datenverarbeitung der jeweiligen Landesrundfunkanstalt vorliegt. Die im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle ist Teil der Landesrundfunkanstalten. Im Übrigen weise ich auf die jeweilige vom Bundesland abhängige Vorschrift zur Meldedatenübermittlung[27] hin, die die Übermittlung von bestimmten Daten an die Landesrundfunkanstalten oder der beauftragten Stelle (Beitragsservice) zu den Zwecken der Erhebung und des Einzugs der Rundfunkbeiträge regelt.

Ich erläutere ergänzend im Rahmen der Beratung, dass auch die im Beschwerdeschreiben platzierte Aufforderung, eine automatisierte Entscheidung nach Art. 22 Abs. 1 DSGVO zu unterlassen, nach unserer Überzeugung nicht greift, da es bei der Meldedatenübermittlung bereits an einer tatbestandlich erforderlichen Entscheidung[28] fehlt.

8.4 Verarbeitung von Gesundheitsdaten

Im Berichtsjahr erreichte mich die Beschwerde eines Beitragszahlers, der monierte, vom Beitragsservice aufgefordert worden zu sein, ein augenärztliches Attest vorzulegen. Er zweifelte, auf welcher Rechtsgrundlage diese Datenerhebung erfolgen sollte, weshalb ich den Beitragsservice um Stellungnahme gebeten habe.

Der Beitragsservice erläuterte zunächst, dass der Beschwerdeführer beantragt hatte, künftig Schreiben barrierefrei vom Beitragsservice zu erhalten. Es sei daraufhin gebeten worden, ein

[27] § 23 Bayerische Meldedatenverordnung (BR), § 7 Meldedatenübermittlungsverordnung NRW (WDR), § 5 Saarl. Bundesmeldegesetz- Ausführungsgesetz (SR), § 7 Bundesmeldegesetz Ausführungsgesetz LSA (MDR), § 13 Meldeverordnung BW (SWR), § 12 Meldedatenlandesverordnung Rheinland-Pfalz (SWR), § 18 Meldedaten-übermittlungsverordnung Hessen (HR), § 8 Meldedatenübermittlungsverordnung Brandenburg (rbb), § 3 Berliner Meldedatenverordnung (rbb)

[28] Siehe hierzu beispielhaft Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 22 Rn. 15a-15c: „Der Anwendungsbereich des [Art.22] Abs. 1 [DSGVO] erfasst nicht generell jeden auf einer automatisierten Verarbeitung beruhenden Vorgang, sondern lediglich Entscheidungen. Die Vorschrift begrenzt ihre Anwendung damit auf gestaltende Akte, die eine Wahl zwischen mindestens zwei Alternativen treffen und eine Wirkung in der Außenwelt erzielen, die über das Forum internum hinausreicht. Erforderlich sind also typischerweise ein Regelungswille und eine Willensäußerung […].

augenärztliches Attest vorzulegen, um nachzuweisen, dass er aufgrund einer Sehbehinderung auf die Bereitstellung von Schriftstücken in barrierefreier Form angewiesen ist. Der Beitragsservice hat sich zunächst dahingehend eingelassen, dass die Erforderlichkeit eines solchen Nachweises damit zu begründen sei, dass die Übersendung von Dokumenten in barrierefreier Form mit erheblichem technischem und verwaltungsorganisatorischem Mehraufwand verbunden sei.

Ausgehend dieser Begründung habe ich gegenüber dem Beitragsservice Zweifel angemeldet hinsichtlich der Rechtsgrundlage zur Verarbeitung von Gesundheitsdaten (hier das ärztliche Attest), denn im Rundfunkbeitragsstaatsvertrag ist eine solche Verarbeitung nicht vorgesehen, und auch nach Maßgabe des Art. 9 DSGVO müsste eine ausdrückliche Einwilligung eingeholt oder begründet werden, inwieweit die Verarbeitung erforderlich ist, um z.B. eine Rechtausübung gem. Art. 9 Abs. 2 lit. b DSGVO zu ermöglichen. Anders ausgedrückt, es müsste sich aus einem Gesetz ergeben, dass die Erhebung von Gesundheitsdaten für den vom Beitragsservice genannten Zweck gesetzlich vorgesehen und damit auch erforderlich ist.

Der Beitragsservice hat sich meiner Rechtsauffassung angeschlossen und angekündigt, dass Verfahren anzupassen, damit dem Wunsch nach barrierefreier Kommunikation auch ohne ärztliche Atteste oder sonstige gesundheitliche Nachweise entsprochen wird. Formen solcher Kommunikation können bspw. Großdruck, Datenträger per Post, Schreiben in Blindenschrift o.ä. sein. Eine Begründung der Erhebung von Gesundheitsdaten nur aus dem Grund, dass barrierefreie Kommunikation einen erheblichen Aufwand nach sich zieht, ist nicht statthaft und vom Datenschutzrecht nicht gedeckt. Ebenso hat der Beitragsservice darauf hingewiesen, dass es im Rahmen der Sachbearbeitung bereits eine Regel gibt, die das Anfordern von Gesundheitsdaten oder ärztlichen Attesten bei dem Wunsch nach barrierefreier Kommunikation ausschließt. Insofern ist in diesem Fall davon auszugehen, dass es sich um einen Einzelfall handelte.

Dennoch – und dies muss sich auch der Beitragsservice stets vor Augen führen – ist im Bereich von Gesundheitsdaten mit großer Sorgfalt vorzugehen. Der Beitragsservice hat infolgedessen Sensibilisierungsmaßnahmen für die Mitarbeitenden der Sachbearbeitung ergriffen; auch gegenüber dem Beschwerdeführer wurde der Fehler eingeräumt und um Entschuldigung gebeten.

Im Ergebnis halte ich dieses Vorgehen für angemessen und damit ausreichend, weshalb ich von weiteren aufsichtsrechtlichen Maßnahmen in dieser Angelegenheit absehen konnte.

8.5 Löschung von Bankdaten

Mit Unverständnis reagieren manche Beschwerdeführer auf die Tatsache, dass der Beitragsservice auch alte und ggf. nicht mehr genutzte Bankverbindungsdaten in seinem Bestand aufbewahrt. Oft wird auf Art. 17 der Datenschutzgrundverordnung hingewiesen, wonach personenbezogene Daten

dann zu löschen sind, wenn diese für die Zwecke, für die sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr notwendig sind.

Ich nutze die Gelegenheit, den Betroffenen kurz zu erläutern, dass der Beitragsservice im Zuge der Überweisung des Rundfunkbeitrags auch die dafür genutzten Daten zur Bankverbindung erhält.

Neben solchen aus dem Rundfunkbeitragsstaatsvertrag ergeben sich Verpflichtungen aus anderen Gesetzen zur Verarbeitung von Daten, insbesondere aus den einschlägigen Regelungen des Handelsgesetzbuches (HGB) bzw. aus den Grundsätzen der ordnungsgemäßen Buchführung. Diese Vorschriften bilden auch die konkrete Rechtsgrundlage dafür, dass die Bankverbindungdaten auch im Falle einer Einzelüberweisung verarbeitet, also gespeichert bzw. aufbewahrt werden müssen.

Nach den Grundsätzen der ordnungsgemäßen Buchführung besteht die Anforderung, dass jede Zahlung konkret nachvollzogen werden musss und damit ein sogenannter Buchungsbeleg vorzuhalten ist. Hierzu gehört die Speicherung der Bankdetaildaten desjenigen, der Zahlungen an die Landesrundfunkanstalt leistet. Bisherige Bankverbindungen oder auch Kontodaten von Einzelüberweisungen müssen im Rahmen der Aufbewahrungspflicht vom Beitragsservice gespeichert werden.

Vereinzelt wird mir dann entgegengehalten, der Beitragsservice sei nicht nach handelsrechtlichen Vorschriften verpflichtet, die Bankverbindungsdaten der Rundfunkbeitragszahler zu speichern. Diesem Einwand ist zu entgegnen, dass der Beitragsservice als eine nichtrechtsfähige Verwaltungsgemeinschaft von den öffentlich-rechtlichen Landesrundfunkanstalten, ZDF und Deutschlandradio gemeinsam betrieben wird. Folglich sind die rechtlichen Vorgaben bei den Landesrundfunkanstalten zu beachten. Beispielhaft kann hier verwiesen werden auf den § 30 Abs. 3 MDR-Staatsvertrag sowie auf § 41 Abs. 2 WDR-Gesetz, wonach der Jahresabschluss nach den Bestimmungen des Handelsgesetzbuches für große Kapitalgesellschaften aufzustellen ist. Die Landesrundfunkanstalten haben davon ausgehend den Beitragseinzug geregelt und die Grundlagen des Verfahrens festgelegt. Dies umfasst die Beachtung der einschlägigen handelsrechtlichen Vorgaben. Abrundend verweise ich auf die §§ 238, 257 Abs. 4 HGB, die eine Aufbewahrung von Buchungsbelegen konkret vorschreiben.

Ausgangspunkt dieser Fragen ist im Übrigen häufig, dass der Auskunftsanspruch aus § 11 Abs. 8 Rundfunkbeitragsstaatsvertrag auch vorsieht, die Bankverbindungsdaten dem Auskunftsersuchenden mitzuteilen. Der Beitragsservice ist der Auffassung – und meiner Ansicht nach zurecht, dass dies auch die nicht mehr genutzten, aber aufbewahrungspflichtigen Bankverbindungsdaten umfasst. Insofern ist verständlich, dass manche Beitragszahlerinnen und Beitragszahler von Zeit zu Zeit wissen möchten, warum nicht mehr zum Beitragseinzug genutzte Daten vorgehalten werden müssen.

8.6 Datenweitergabe an Gerichtsvollzieher

Im Berichtsjahr erreichten mich zahlreiche gleichlautende Beschwerden, die eine Weitergabe von persönlichen Daten an Vollstreckungsbehörden und Gerichtsvollzieher bemängelten. Es wurde in empörtem Duktus die Auffassung vertreten, der Beitragsservice sei nicht befugt, Vollstreckungsmaßnahmen zu ergreifen, da es sich lediglich um eine Inkassostelle und keine Behörde handele.

Ich habe im Wesentlichen und gleichlautend darauf geantwortet, dass der nach meinem Dafürhalten wahrscheinliche Anlass der Beschwerden ein vom Beitragsservice festgestellter Rückstand an Beitragszahlungen gewesen sein dürfte, zu dem ein Festsetzungsbescheid ergangen sei. Dies konnte ich der Einlassung aller Beschwerdeführer entnehmen, einen Festsetzungsbescheid verwaltungsgerichtlich angegriffen zu haben.

So war für mich zunächst festzustellen, dass es im Kern um die Klärung eines Beitragssachverhalts und nur nachrangig um eine datenschutzrechtliche Frage ging. Ich habe ausführlich erläutert, dass der Beitragsservice befugt ist, Festsetzungsbescheide im Verwaltungsvollstreckungsverfahren durch eine zuständige Vollstreckungsbehörde durchsetzen zu lassen; dies setzt notwendigerweise die Übermittlung der entsprechenden personenbezogenen Daten an diese voraus. Ebenso habe ich versucht zu verdeutlichen, dass die mit der Abwicklung eines Beitragsverhältnisses verbundene Datenverarbeitung, einschließlich der Weitergabe personenbezogener Daten an Vollstreckungsbehörden, lediglich die notwendige Folge eines tatsächlichen oder vermeintlichen Verstoßes gegen die Beitragspflicht sei. Ich habe nicht zu entscheiden, ob der Beitragsservice in den konkreten Fällen zu Recht einen Zahlungsrückstand festgestellt und das Vollstreckungsverfahren eingeleitet hat. Eine entsprechende Überprüfung ist nicht Sache der Datenschutzaufsicht, sondern muss im Rahmen eines Widerspruchs bzw. eines verwaltungsgerichtlichen Klageverfahrens gegen den zugrunde liegenden Beitragsfestsetzungs- bzw. Vollstreckungsbescheid geklärt werden. Eingreifen kann ich nur dann, wenn es Anhaltspunkte dafür gibt, dass der Beitragsservice offenkundig fehlerhaft vom Bestehen einer Beitragspflicht bzw. von einem Zahlungsrückstand im konkreten Fall ausgegangen ist und die Datenweitergabe an die Vollstreckungsstelle deshalb erkennbar rechtsgrundlos veranlasst wurde.

Keinem der mir geschilderten Sachverhalte haben sich solcherlei Anhaltspunkte entnehmen lassen. Ich habe die Beschwerdeführenden deswegen gebeten, entsprechende Angaben nachzureichen, die mir eine vollständige Beurteilung auch des Beitragssachverhalts zumindest in groben Zügen ermöglicht hätte. Dies ist in keinem Fall geschehen, ebenso gab es zu meinen ausführlichen Antworten in der Sache keinerlei Reaktionen. Ich gehe daher davon aus, dass es sich bei diesen Beschwerden um Muster handelt, die von Beitragszahlerinnen und Beitragszahlern wohl in Unkenntnis der tatsächlichen Rechtslage an den Rundfunkdatenschutzbeauftragten gesandt wurden. Insofern erwiesen sich die Eingaben allesamt als unbegründet.

8.7 Adresshandel

Wiederholt gingen Anfragen oder Beschwerden ein, die sich mit der Nutzung von Adressdaten auseinandersetzen, die der Beitragsservice von Adresshändlern bezogen hat.

Zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten von Adresshändlern weise ich sodann auf § 11 Abs. 4 Rundfunkbeitragsstaatsvertrag (RBStV) hin. Danach verarbeitet die zuständige Landesrundfunkanstalt für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach dem RBStV besteht, personenbezogene Daten bei öffentlichen und nichtöffentlichen Stellen ohne Kenntnis der betroffenen Person. Als „Nichtöffentliche Stellen“ definiert die Regelung „Unternehmen des Adresshandels und der Adressverifizierung.“

Voraussetzung für eine solche Verarbeitung ist gleichwohl, dass gemäß § 11 Abs. 4 S. 5 RBStV (1.) eine vorherige Datenerhebung unmittelbar bei der betroffenen Person erfolglos war oder nicht möglich ist, (2.) die Datenbestände dazu geeignet sind, Rückschlüsse auf die Beitragspflicht zu zulassen, insbesondere durch Abgleich mit dem Bestand der bei den Landesrundfunkanstalten gemeldeten Beitragsschuldner, und (3.) sich die Daten auf Angaben beschränken, die der Anzeigepflicht nach § 8 unterliegen und kein erkennbarer Grund zu der Annahme besteht, dass die betroffene Person ein schutzwürdiges Interesse an dem Ausschluss der Verarbeitung hat.

Der Beitragsservice ist damit grundsätzlich befugt, Adressdaten anzukaufen. Dies bezieht sich gem. § 14 Abs. 9 RBStV allerdings nicht auf Adressdaten privater Personen, sondern nur auf solche im nicht privaten Bereich, z.B. von Gewerbebetrieben und auch von Selbstständigen. Hintergrund ist, dass im nichtprivaten Bereich „die Aktualität des Datenbestandes nicht im Wege des Meldedatenabgleichs nach § 11 Abs. 5 [RBStV] sichergestellt werden [kann], da mit diesem Instrument lediglich private Meldedaten übermittelt werden“[29].

Die von § 11 Abs. 4 S. 5 Ziff. 3 RBStV vorzunehmende Abwägung mit dem schutzwürdigen Betroffeneninteresse stellt in den allermeisten Fällen keine Hürde dar, da die Eingriffsintensität eines Klärungsschreibens als äußerst gering eingestuft werden kann. Wurde die Anmeldepflicht durch einen möglicherweise Beitragspflichtigen verletzt, ist sein „Interesse, verschont zu bleiben“, nicht schützenswert.

Die konkrete Zweckbestimmung dieser Datenverarbeitung ist im Staatsvertrag damit klar geregelt (hier: Feststellung, ob eine Beitragspflicht nach dem RBStV besteht, vgl. § 11 Abs. 4 S. 1. RBStV) und bezüglich der Datenweitergabe der Adresshändler an den Beitragsservice auf das für diesen Zweck

[29] BWLT-Drs. 16/7779, 18; siehe auch: Beck RundfunkR/Göhmann/Herb/Siekmann, 5. Aufl. 2024, RBeitrStV § 14 Rn. 50

notwendige Maß beschränkt. Die Erhebung der Adresse ist im Übrigen nach § 11 Abs. 4 S. 5 Ziff. 3 i.V.m. § 8 RBStV vorgesehen.

Die Richtigkeit dieser Daten ist vorab allerdings nicht überprüfbar und kann nur im Rahmen einer Klärung mit dem Betroffenen erfolgen. Im Zusammenhang mit dem dann durchgeführten Klärungsverfahren entstehen in der Regel die Fragen der Petenten, die sich dann mit Anfragen zur Rechtmäßigkeit dieser Datenverarbeitung an mich wenden.

In den Datenschutzhinweisen des Beitragsservice zum Beitragseinzug wird überdies unter der Überschrift „Aus welchen Quellen stammen die Daten?“ beschrieben, woher die Daten stammen, die der Beitragsservice erhält. Ein transparenter Hinweis des Beitragsservice auf diese Form der Datenverarbeitung ist somit vorhanden.

9 Rundfunkdatenschutzkonferenz (RDSK)

Die Rundfunkdatenschutzbeauftragten haben sich in der Rundfunkdatenschutzkonferenz (RDSK) zusammengeschlossen. Im Berichtsjahr bestand die RDSK aus vier Personen, die die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk über die Rundfunkanstalten und deren Gemeinschaftseinrichtungen und Beteiligungsunternehmen ausüben. Die Mitglieder der RDSK können dem Anhang 13.6 entnommen werden. Im Berichtsjahr haben Sitzungen der RDSK am 16.04.2024, am 30.07.2024 und am 27.11.2024 stattgefunden. Den Vorsitz im Berichtsjahr habe ich übernommen und die Stellvertretung Herr Dr. Neuhoff, der Rundfunkdatenschutzbeauftragte beim Norddeutschen Rundfunk. In der Sitzung am 27.11.2024 wurde ich erneut zum Vorsitzenden gewählt. Die weiteren Mitglieder der RDSK übernahmen gleichermaßen die Stellvertretung.

9.1 Aufgaben der RDSK

Die Aufgaben der RDSK sind festgehalten in der Geschäftsordnung, die sich die RDSK 2019 gegeben hat. Die RDSK soll einen Beitrag zur einheitlichen Anwendung der DSGVO in den Rundfunkanstalten leisten. Die Mitglieder arbeiten unter Wahrung der jeweiligen Unabhängigkeit eng zusammen und tauschen sich aus. Neben der Geschäftsordnung wurden 2023 die Verwaltungsvereinbarungen zur Wahrnehmung der Datenschutzaufsicht über die Gemeinschaftsunternehmen der Rundfunkanstalten und zur Wahrnehmung der Datenschutzaufsicht über

Gemeinschaftseinrichtungen zu einer Verwaltungsvereinbarung zusammengefasst, die Anfang 2024 in Kraft trat. [30].

Die RDSK-Veröffentlichungen und grundsätzliche Themen sind auf der Homepage der Rundfunkdatenschutzkonferenz unter www.rundfunkdatenschutzkonferenz.de abzurufen.

In den Sitzungen der RDSK wurde schwerpunktmäßig über folgende Themen beraten:

- Zusammenarbeit mit der DSK
- Berichte aus dem AK Medien, dem AK Grundsatz, dem AK Technik
- regelmäßiger Austausch mit den staatlichen Aufsichten und erstmaliger Austausch mit Datenschutzaufsichten der privaten Medien
- Nutzungsmessung, insbesondere mit Schwerpunktthema Anonymisierung
- Orientierungshilfe zum datenschutzkonformen Einsatz von KI im öffentlich-rechtlichen Rundfunk (Erarbeitung von Nachschärfungen und Aktualisierungen, Versionen 2.0 und 2.1)
- Datenschutzfolgenabschätzungen – Liste Art. 35 Abs. 4 und 5 DSGVO
- Grundlagen für die Verhängung von Bußgeldern gem. Art. 58 Abs. 2 lit. i DSGVO
- Aktualisierung der Empfehlungen zum Einsatz von Cookies und Local Storage-Elementen (TDDDG)
- Inhaltsgleiche Vollstreckungsbeschwerden über den Beitragsservice
- Reichweite des Medienprivilegs und Umgang mit dem Datengeheimnis
- Informationstiefe zur Auftragsverarbeitung
- Aufzeichnung von Betriebs-/Personalversammlungen
- Hinweisgeberschutz
- Reformstaatsvertrag (MStV-Entwurf)

Auch wenn sich die RDSK in den letzten Jahren personell verkleinert hat, so hat sie nichts von ihrer Wichtigkeit eingebüßt. Der Austausch mit den Kolleginnen und Kollegen unter Aufsichtsgesichtspunkten ist gerade in Ergänzung zur Zusammenarbeit mit dem AK DSB von eigenständiger Bedeutung. Im Berichtsjahr hat sich erneut gezeigt, dass die RDSK schnell auf aktuelle Entwicklungen und datenschutzrechtliche Themen reagieren kann. Gerade die rasche Erstellung und Aktualisierung der Orientierungshilfe zum datenschutzkonformen Einsatz von KI sowie die Stellungnahmen zu Bußgeldern und Datenschutzfolgenabschätzungen haben erwiesen, dass die Zusammenarbeit in der RDSK gut funktioniert und für die Praxis in den Rundfunkanstalten wichtig ist. In Zukunft könnten sich Veränderungen der RDSK durch die Umsetzung des Reformstaatsvertrags ergeben.

[30] Siehe Kapitel 13.7 im Anhang

9.2 Handreichungen, Empfehlungen und Orientierungshilfen

Nach der Geschäftsordnung der Rundfunkdatenschutzkonferenz erarbeitet und veröffentlicht die RDSK Orientierungshilfen, Handreichungen sowie Positionspapiere zu inhaltlichen, technischen oder organisatorischen Fragen des Datenschutzes. Folgende Papiere wurden im Berichtsjahr erstellt.

9.2.1 Orientierungshilfe KI

Wie in Kapitel 6.4 bereits erwähnt, hat die RDSK die im August 2023 erarbeitete Orientierungshilfe im Jahr 2024 an aktuelle Entwicklungen angepasst und nachgeschärft, indem Erfahrungen und Anregungen aus der Praxis der Rundfunkanstalten aufgegriffen werden konnten. Die im September 2024 veröffentlichte Version 2.1 der Orientierungshilfe[31] ist im Ergebnis anwendungsfreundlicher und verständlicher geworden. Insbesondere soll die beigefügte Checkliste auf den ersten Blick über Wichtiges informieren und für die zu beachtenden wesentlichen Schritte vor und beim Einsatz von KI im öffentlich-rechtlichen Rundfunk sensibilisieren.

Ich bin auch weiterhin dankbar für jegliche Anmerkungen und Fragen zur Auslegung dieser Orientierungshilfe. Die Entwicklungen werden weiter rasant voranschreiten, sodass davon auszugehen ist, dass weitere Aktualisierungen in Zukunft erforderlich werden.

Die Orientierungshilfe soll neben der Information über (datenschutz-)rechtliche Hintergründe und Maßgaben beim Einsatz von KI über Risiken aufklären sowie konkrete Handlungsanweisungen je nach Einsatzgebiet im öffentlich-rechtlichen Rundfunk geben.

Auf die wesentlichen Erwägungen soll hier kurz eingegangen werden:

Zunächst werden die Regelungen der seit 01.08.2024 in Kraft getretenen KI-Verordnung skizziert und dabei die zum Verständnis wichtige Unterscheidung von KI-Modellen und KI-Systemen erläutert.

Anschließend wird grundlegend auf die datenschutzrechtlichen Maßgaben eingegangen. Wie auch bei anderen Anwendungen, in denen personenbezogene Daten verarbeitet werden, muss bei KI-Anwendungen zunächst der Zweck des Einsatzes eines KI-Systems und die Notwendigkeit der damit einhergehenden Datenverarbeitung so genau wie möglich beschrieben werden. Transparenzgesichtspunkte spielen stets eine große Rolle, dazu gehören die Zugänglichmachung

[31] https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/orientierungshilfen/orientierungshilfe-zum-datenschutzkonformen-einsatz-von-ki-im-oeffentlich-rechtlichen-rundfunk

und Anpassung von Datenschutzerklärungen und ggf. Einwilligungstexten. Obligatorisch ist auch die Etablierung technischer und organisatorischer Maßnahmen, um den Anforderungen der Datensicherheit zu genügen. Ggf. sind vertragliche Rahmenbedingungen in Form von Auftragsverarbeitungsverträgen zu gestalten. Unumgänglich ist es, eine Rechtsgrundlage für die konkrete Verarbeitung zu finden, wie sie in Art. 6 Abs. 1 DSGVO zur Auswahl stehen.

Als besonders relevant für die Risikoabwägung und datenschutzrechtliche Würdigung hat sich im Nachgang der ersten Version der Orientierungshilfe die Frage gezeigt, ob die eingesetzten Systeme offen oder geschlossen sind, hier wurde entsprechend nachgeschärft. Geschlossene Systeme verarbeiten Daten nur in einer begrenzten technisch abgeschlossenen Umgebung. Im Papier wird deutlich gemacht, dass das auch eine abgeschlossene Cloud-Infrastruktur sein kann. Ein Zugriff auf die im geschlossenen System verarbeiteten Daten durch das frei zugängliche Internet ist ausgeschlossen. Damit fließen die Daten nicht in das allgemeine Training des KI-Systems ein, lediglich ein Training innerhalb des geschlossenen Systems ist möglich. Offene Systeme werden dagegen über das frei zugängliche Internet betrieben und durch einen unbestimmten Personenkreis trainiert. Das Risiko, dass personenbezogene Daten dann zu anderen Zwecken weiterverarbeitet und an anderer Stelle offengelegt werden, wird mangels Kontrolle und Transparenz als hoch eingeschätzt.

Eine Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO ist zusätzlich immer dann erforderlich, wenn besondere und hohe Risiken für die Rechte und Freiheiten der betroffenen Personen zu befürchten sind.

Neben den Risiken beim Einsatz von KI, wie z.B. mangelnde oder gar fehlende Transparenz im Hinblick auf die mit der KI verbundene Datenverarbeitung und die Erfüllung der Informationspflichten gegenüber den betroffenen Personen, wird darauf hingewiesen, dass die Betroffenenrechte wie Auskunfts- oder Löschungsersuchen erfüllt werden können müssen. Schließlich muss die Frage gestellt werden, wo die Datenverarbeitung stattfindet, insbesondere bei Datenübertragungen in Länder außerhalb der EU.

Ein weiterer Schwerpunkt der Orientierungshilfe war die Frage, welche Verantwortungssphären sich beim Einsatz von KI ergeben: Kann eine Auftragsverarbeitung angenommen werden, muss anderenfalls eine gemeinsame Verantwortung für die in der KI stattfindende Datenverarbeitung festgestellt werden oder besteht eine getrennte Verantwortung? Die RDSK hat geraten, die Verantwortung möglichst vollständig zu übernehmen, da der Zweck der Datenverarbeitung im Wesentlichen die journalistische Datenverarbeitung sein dürfte. Insofern ist es sehr ratsam, einen Auftragsverarbeitungsvertrag abzuschließen, wenngleich das Medienprivileg den Abschluss einer solchen Vereinbarung im journalistischen Kontext nicht obligatorisch fordert. Damit ist aber

sichergestellt, dass die Rundfunkanstalten als Verantwortliche den größtmöglichen Einfluss auf die in der KI stattfindende Datenverarbeitung behalten. Die RDSK hat darauf hingewiesen, dass eine KI-Datenverarbeitung sofort gestoppt werden muss, sobald Anhaltspunkte ersichtlich sind, dass Daten nicht zweckgebunden und vertragsgemäß durch den KI-Anbieter verarbeitet werden.

Die Orientierungshilfe listet schließlich schlagwortartig verschiedene Punkte auf, die beim Einsatz von KI beachtet werden müssen, um den Bereichen der Rundfunkanstalten - insbesondere den Redaktionen - eine gewisse Sicherheit zu geben.

Um einen Einsatz von KI rechtssicher zu ermöglichen, ist im journalistischen Kontext u.a. Folgendes zu beachten:

KI-Anwendungen (auch offene Systeme) können redaktionelles Arbeitsmittel und/oder Berichtsgegenstand sein. Die eingesetzten Systeme dürfen die Einhaltung des Datengeheimnisses nicht gefährden und die Grundsätze der Vertraulichkeit und Integrität zur Gewährleistung der Datensicherheit nicht verletzen. Die in offene KI-Anwendungen eingespeisten Inhalte dürfen daher nicht vertraulich sein. Beim Einsatz von KI sind die Programmgrundsätze zu wahren. Auch bei KI-generierten Programmangeboten gilt die journalistische Sorgfaltspflicht. Die Persönlichkeitsrechte betroffener Personen sind auch beim Einsatz von KI zu beachten und Kinder genießen einen besonderen Schutz. Nicht vergessen werden darf: Die von KI-Anwendungen verarbeiteten Daten können urheberrechtlich geschützt sein. Die Vorgaben des Urheberrechts gelten auch beim Einsatz von KI.

Auch beim Einsatz für unternehmensinterne Zwecke (Verwaltung) sind Regeln zu beachten:

So ist zu bedenken, dass interne, vertrauliche und streng vertrauliche Informationen nicht in offene KI-Systeme eingespeist werden dürfen. Dazu gehören interner Schriftverkehr, Korrespondenzen mit Geschäftspartnern, Beschäftigtendaten (etwa Daten zu Einkommen, Bewerbungsunterlagen, etc.) oder auch Geschäftsgeheimnisse (z. B. streng vertrauliche Revisionsberichte). Offene KI als Arbeitsmittel für unternehmensinterne Zwecke kann mithin nur für solche Informationen eingesetzt werden, die ohnehin öffentlich sind (dies sind z. B. öffentlich erreichbare Internetseiten, öffentlich zugängliche Verzeichnisse oder andere öffentlich zugängliche Quellen wie Pressemitteilungen/frei zugängliche Medienangebote). Der Einsatz von geschlossenen KI-Systemen (z.B. On-Premise oder Private-Cloud) ist vorzugswürdig, da die verarbeiteten Daten dann nicht in das Training der KI einfließen.

9.2.2 Listen zur Datenschutzfolgenabschätzungen

Im August 2024 veröffentlichte die RDSK einen Beschluss zur in Art. 35 Abs. 4 DSGVO niedergelegten Erforderlichkeit einer aufsichtsrechtlichen Erstellung einer Liste der Verarbeitungsvorgänge, für die eine Datenschutzfolgenabschätzung vom Verantwortlichen vorzunehmen ist (sogenannte Blacklist) und zur optionalen Möglichkeit gemäß Art. 35 Abs. 5 DSGVO der Erstellung einer Liste für Verarbeitungsvorgänge, für die ausdrücklich keine Datenschutzfolgenabschätzung vorzunehmen ist (sogenannte Whitelist).[32]

Die RDSK vertritt die Auffassung, dass ein Bedarf an gesonderten, nur für den öffentlich-rechtlichen Rundfunk geltenden Listen gemäß Art. 35 Absatz 4 und 5 DSGVO derzeit nicht besteht. Grund hierfür ist, dass die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine gemeinsame Liste für Datenverarbeitungen im nicht-öffentlichen Bereich nach Art. 35 Absatz 4 DSGVO verabschiedet hat. Die Liste erfasst solche Verarbeitungstätigkeiten, die regelmäßig auch in den Rundfunkanstalten und ihren Beteiligungsunternehmen vorgenommen werden. Die Mitglieder der Rundfunkdatenschutzkonferenz haben daher beschlossen, diese Liste für den jeweilig beaufsichtigten Zuständigkeitsbereich anzuwenden. Auch im Sinne der vom Gesetzgeber intendierten Harmonisierung der Auslegung und Anwendung datenschutzrechtlicher Vorgaben konnte von der Erstellung gesonderter Listen abgesehen werden. Soweit zur Erfüllung des Auftrags des öffentlich-rechtlichen Rundfunks Bereichsausnahmen von datenschutzrechtlichen Regelungen erforderlich sind (Medienprivileg), gelten die in Art. 85 DSGVO genannten Ausnahmen in der Ausformung des nationalen Rechts.

9.2.3 Grundlagen für die Verhängung von Bußgeldern

Ebenfalls im August 2024 veröffentlichte die RDSK eine Stellungnahme über die „Grundlagen für die Verhängung von Bußgeldern gemäß Art. 58 Abs. 2 lit. i DSGVO.[33] Darin erinnert die RDSK daran, dass die Datenschutzaufsichten über den öffentlichen Rundfunk keine Befugnis haben, Geldbußen im Sinne des Art. 58 Abs. 2 lit. i DSGVO gegen die Rundfunkanstalten zu verhängen. Entsprechende Regelungen finden sich in den Staatsverträgen der Landesrundfunkanstalten (z.B. § 46 Abs. 1 S. 4 NDR-Staatsvertrag). Die Befugnisse der Datenschutzaufsichten nach Art. 58 DSGVO sind jedoch nicht beschränkt, wenn es sich um Beteiligungsunternehmen der Rundfunkanstalten handelt. Aufgrund der Marktteilnahme dieser Unternehmen kommt im Falle eines Verstoßes gegen

[32] https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/beschluesse/datenschutzfolgenabschaetzungen-liste-art-35-abs-4-und-5-dsgvo-august-2024
[33] https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/stellungnahmen-entschliessungen/grundlagen-fuer-die-verhaengung-von-bussgeldern-gem-art-58-abs-2-lit-i-dsgvo-august-2024

datenschutzrechtliche Vorgaben auch die Aufsichtsmaßnahme des Art. 58 Abs. 2 lit. i DSGVO – mithin die Verhängung einer Geldbuße – in Betracht.

Entsprechend der Leitlinien zur Bußgeldzumessung des Europäische Datenschutzausschusses (EDSA) aus dem Jahr 2023 folgt die Verhängung von Bußgeldern nun einem im Geltungsbereich der DSGVO einheitlichen Konzept. Aufgrund der europaweiten Harmonisierung werden auch die Aufsichtsbehörden über den öffentlich-rechtlichen Rundfunk die Leitlinien zur Bußgeldzumessung anwenden.

10 Arbeitskreis der Datenschutzbeauftragten (AK DSB)

Der AK DSB existiert seit 1979, und in diesem Kreis treffen sich die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten. Hinzugekommen sind die Datenschutzbeauftragten des ORF aus Österreich und auch der SRG aus der Schweiz. Zweimal im Jahr finden reguläre Sitzungen in Präsenz statt, dazwischen werden zu wichtigen Themen Videokonferenzen anberaumt. Den Vorsitz im Berichtsjahr hatte die behördliche Datenschutzbeauftragte des Beitragsservice inne, ihre Stellvertreterin war die Datenschutzbeauftragte des WDR.

10.1 Organisatorische Weiterentwicklung

Das Jahr 2024 stand im Zeichen der Weiterentwicklung des AK DSB, und zwar im Hinblick auf seine Rolle, die Organisation sowie die Abgrenzung zu und die Zusammenarbeit mit anderen Gremien.

Die Bestimmung von Unterarbeitsgruppen, die sich stellvertretend für alle AK DSB-Mitglieder spezifischen Themen widmen und bei den AK DSB-Sitzungen über deren Arbeitsfortschritt berichten, war ein wichtiger Schritt in Richtung einer effizienten und zielgerichteten Zusammenarbeit.

Beschlossen und umgesetzt wurde weiterhin ein einheitliches Erscheinungsbild des AK DSB. Ein Logo wurde gestaltet, um die Identität und die Wiedererkennung des AK DSB zu stärken.

10.2 Austausch im AK DSB

Als Rundfunkdatenschutzbeauftragter bei insgesamt neun Rundfunkanstalten nehme ich nach wie vor an den Sitzungen teil. Es hat sich gezeigt, dass der Austausch mit den internen

Datenschutzbeauftragten neben den vierteljährlichen Jour fixes wichtig ist. Themen, die den betrieblichen Datenschutz und somit die datenschutzrechtliche Praxis in den Rundfunkanstalten betreffen, werden regelmäßig im AK DSB besprochen, und so sind die Sitzungen auch eine Quelle der Erkenntnis, auf die ich nur ungern verzichten würde. Nachvollziehbar ist für mich aber dennoch, dass die Aufsicht nicht in alle Themen einbezogen werden sollte oder gar muss. Um meinem eigenen Anspruch gerecht zu werden, auch individuell die Rundfunkanstalten in den Blick zu nehmen, fühle ich mich dennoch aufgerufen, weiterhin an den Sitzungen des AK DSB teilzunehmen und dort einen Beitrag zu leisten.

Im Berichtsjahr wurden u. a. folgende Themen diskutiert

- Grundfragen zu Rolle und Organisation des AK DSB
- Umsetzung von Gemeinschaftsprojekten durch mehrere Rundfunkanstalten und die prozessuale Einbeziehung des AK DSB in eine datenschutzrechtliche Beratung
  - Datenschutzthemen im Rahmen einer geplanten Harmonisierung der technischen Infrastruktur der Rundfunkanstalten
- KI und Möglichkeiten einer datenschutzkonformen Nutzung
- Datenschutzrechtliche Bewertung von M365-Anwendungen
- Nutzungsmessung in den Rundfunkanstalten
- Vereinheitlichung von Vorlagen für datenschutzrechtliche Prozesse
- Überwachungsaufgaben der Datenschutzbeauftragten

11 Austausch mit der Datenschutzkonferenz (DSK)

Die Datenschutzaufsichtsbehörden der Länder und ebenso die Bundesdatenschutzbeauftragte müssen nach dem Bundesdatenschutzgesetz in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der DSGVO zusammenarbeiten. In diesem Zusammenhang sind auch die nach Art. 85 und 91 der DSGVO eingerichteten Aufsichtsbehörden zu beteiligen. Daher treffen Vertreterinnen und Vertreter der Bundesdatenschutzbeauftragten, der Landesdatenschutzbeauftragten mit den Rundfunkdatenschutzbeauftragten, den Aufsichten über den privaten Rundfunk sowie den Aufsichten der evangelischen und katholischen Kirche zusammen. Diese Treffen finden regelmäßig zweimal im Jahr statt. Im Berichtsjahr 2024 am 06. Juni und am 20. November.

Wiederkehrend wird seitens der staatlichen Aufsichtsbehörden aus der Datenschutzkonferenz berichtet und ebenso aus dem Europäischen Datenschutzausschuss. Themen waren u.a.

- Digitalzwang
- Leitlinien zum Datenschutz bei Minderjährigen
- Aufsichtsrechtliche Fragen in Anwendung der KI-Verordnung

Ebenso wurde über Haltung der DSK und der RDSK zum Einsatz von KI gesprochen, im Wesentlichen scheint es hier übereinstimmende Auffassungen zu geben. Mittlerweile gibt es einen Arbeitskreis Künstliche Intelligenz der DSK, an dem auch Vertreter der sogenannten „spezifischen" Aufsichtsbehörden beteiligt werden, also auch der RDSK.

Immer noch beschäftigen wir uns zudem mit dem Thema, wie die Aufsichten des Rundfunks und der Kirchen als vollwertige Aufsichtsbehörden mit der DSK zusammenarbeiten können. Daher wurde im Rahmen der Sitzung am 20.11.2024 darüber beraten, wie konkrete Vereinbarungen über eine effektive Zusammenarbeit gestaltet sein könnten. Seitens der RDSK wurde die Einräumung eines Gaststatus für einen Vertreter der RDSK im Rahmen der DSK, die Mitarbeit in verschiedenen Arbeitskreisen (wobei sämtliche Beratungsunterlagen und der vorbereitende Schriftverkehr vollständig mitgeteilt werden) und die Vereinbarung von Kriterien für Angelegenheiten, in denen eine engere Einbindung wünschenswert ist, vorgetragen und zur Abstimmung gestellt. Der Hessische Landesdatenschutzbeauftragte als Vorsitzender der DSK im Berichtsjahr bestätigte, dass auch die „spezifischen" Aufsichtsbehörden solche im Sinne der DSGVO seien und die Arbeitskreise seitens der DSK aufgerufen seien, ihre Arbeitsweisen zu überprüfen. Die Kommunikation solle verbessert werden, ein einheitliches Auftreten aller Aufsichtsbehörden sei wünschenswert; in der DSK werde die Kooperation mit den weiteren Aufsichtsbehörden insgesamt als nicht kritisch gesehen.

Ich habe bisher auf mein Schreiben vom 14.12.2023 an die seinerzeitige Vorsitzende der DSK (Berichtspunkt 9.1 des letztjährigen Tätigkeitsberichts) noch keine Antwort erhalten. Daher habe ich mich Anfang des Jahres 2025 an die neue Vorsitzende der DSK, Frau Meike Kamp - Berliner Beauftragte für Datenschutz und Informationsfreiheit - gewandt, um dieses ständig wiederkehrende Thema vielleicht im Jahr 2025 zu einem befriedigenden Abschluss zu bringen. Ich halte es für wichtig, in die laufende Arbeit der Arbeitskreise einbezogen zu werden, denn eine Mitarbeit nur auf Grundlage der Teilnahme an den Präsenzsitzungen (jeweils zweimal im Jahr) ist nur eingeschränkt gewinnbringend. Eine effektive Mitarbeit oder zumindest die Nachvollziehung der Entscheidungswege ist allein mit dem uneingeschränkten Zugang zur Kommunikation in den Arbeitskreisen möglich. Die RDSK ist sich der Tatsache bewusst, dass aufgrund der nur eingeschränkten Ausstattung der Rundfunkdatenschutzaufsichtsbehörden eine Partizipation an jedem einzelnen Arbeitsschritt gewiss nicht immer möglich sein wird. Dies ist aber aus meiner Sicht auch gar nicht nötig, um an wichtigen Stellen Impulse zu setzen. Dafür wiederum ist aber vollständiger Informationsfluss unabdingbar.

Ich werde meine Bemühungen fortsetzen, die auch von der DSGVO geforderte Zusammenarbeit mit den anderen Aufsichtsbehörden zu intensivieren und hoffe, dass auch die gemeinsamen Anstrengungen mit den Aufsichten der Kirchen zu guten Ergebnissen führen können.

11.1 AK Medien

An der Sitzung des AK Medien am 04./05.03.2024 in Hamburg hat mein juristischer Referent teilgenommen.

Neben den Berichten aus den für den Datenschutz in den Medien relevanten Subgroups des EDSA (Tech Subgroup, Social Media Subgroup, Berlin Group) sowie vom European Case Handling Workshop (ECHW) wurde in einem wissenschaftlichen Vortrag das Studienergebnis zum Modell eines Einwilligungsagenten gemäß § 26 TDDDG und good practices von informierenden Cookie-Bannern dargestellt. Daneben wurde von den Mitgliedern der DSK über Dienste diskutiert, die pseudonyme Netzwerkkennungen als Alternative zur cookie-basierten personalisierten Werbung anbieten.

Eines der Schwerpunktthemen war der Betrieb von WhatsApp-Kanälen hinsichtlich der datenschutzrechtlichen Verantwortlichkeit sowie außerdem WhatsApp Business, zu dem der BfDI über den aktuellen Sachstand der Untersuchungen informierte.

Die Einladung für die zweite Sitzung des Jahres am 16./17.09.2024 hat meine Behörde leider nicht rechtzeitig erreicht, da seitens der DSK eine veraltete Kontaktadresse genutzt wurde, so dass eine Teilnahme aus Termingründen nicht mehr möglich war.

11.2 AK Grundsatz

Der Arbeitskreis Grundsatz der DSK tagt zweimal jährlich, im Berichtsjahr am 24./25. April sowie am 25./26. September. Der Arbeitskreis wird geleitet vom BfDI und beschäftigt sich – wie der Name schon sagt – mit Fragen von grundsätzlicher Bedeutung. An diesen Sitzungen nehme ich persönlich teil, weil mir der Austausch zu diesen Fragen in der Aufsichtspraxis von großer Wichtigkeit erscheint. Dessen ungeachtet habe ich den Eindruck gewonnen, dass nicht selten Spezialfragen diskutiert werden, die eher dem Grenzbereich des Datenschutzrechtes zuzuordnen sind. Auch nehme ich deshalb gern an den Sitzungen teil, weil der Austausch mit den Kolleginnen und Kollegen einerseits, aber auch die Beschäftigung mit dogmatischen Fragen andererseits von Bedeutung für meine Arbeit sind.

Besprochen wurden u.a. Fragen zum Digitalzwang und zur Gewährleistung der analogen Teilhabe, Grundsatzfragen zu Informationspflichten bei Initiativübermittlungen von Daten durch Betroffene und zu Unterauftragsverarbeitern, sowie zur Frage, insoweit exzessiv handelnde Mitarbeitende als Verantwortliche i.S. des Datenschutzes anzusehen sind.

Turnusgemäß berichtet wird überdies aus der Key Provisions Expert Subgroup des EDSA.

Schade ist nach wie vor, dass die Aufsichtsbehörden des Rundfunks und der Kirchen nicht am E-Mail-Verteiler dieses Arbeitskreises beteiligt sind. Somit bleibt nur die Teilnahme an den Sitzungen, deren thematische Genese nur einschränkbar nachvollziehbar ist (siehe hierzu auch Kapitel 11 zur Zusammenarbeit mit der DSK).

11.3 AK Technik

Im Jahr 2024 war es meiner Aufsichtsbehörde durch die Erweiterung des Teams möglich, auch an den Sitzungen des AK Technik der DSK teilzunehmen. Am 16./17.04.2024 besuchte meine Referentin für technisch-organisatorische Themen die als Videokonferenz durchgeführte Sitzung.

Es wurden grundsätzliche technische und organisatorische Datenschutzfragen erörtert. Neben Berichten zur Zusammenarbeit auf europäischer Ebene sowie aus Arbeitsgruppen und Unterarbeitsgruppen des AK Technik findet dort auch ein Erfahrungsaustausch zu verschiedenen Themen statt. Besonders die vorgestellte Erarbeitung von Leitlinien zur Anonymisierung und Pseudonymisierung knüpfte eng an Themen an, die auch meine Behörde beschäftigen.

Im Hinblick auf technische/IT-Themen konnten wir dank einer Empfehlung aus dem Team des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit den wertvollen Kontakt zum „Informationsaustausch der Aufsichtsbehörden zu IT-Laboren“ herstellen. Schwerpunkt dieser Treffen liegt im Wesentlichen auf konkreten, praktischen Themen der IT-Labore. Den Austausch im Rahmen der ersten Teilnahme an der Sitzung vom 23./24.10.2024 in Berlin haben wir als sehr bereichernd empfunden.

Der Besuch der zweiten Sitzung des AK Technik am 24./25.09.2024 in Schwerin war aus organisatorischen Gründen nicht möglich.

11.4 AK KI

In der gebotenen Kürze wird im Vorgriff auf das Jahr 2025 darüber informiert, dass die DSK einen Arbeitskreis Künstliche Intelligenz (AK KI) ins Leben gerufen hat, an dessen konstituierender Sitzung

ich am 23./24. Januar 2025 teilnehmen konnte. Der Arbeitskreis wird sich mit sämtlichen datenschutzrechtlich relevanten Themen zu Künstlicher Intelligenz befassen und sich insbesondere Betroffenenrechten und Transparenz beim Einsatz von KI-Systemen widmen. Im Zuge dessen soll Forschung und Entwicklung von KI im Hinblick auf technische und juristische Entwicklungen beobachtet werden sowie regulatorische Initiativen in der EU und weltweit in den Blick genommen werden.

Zu meinem Bedauern ist es wiederholt nicht gelungen, als vollwertiges Mitglied dieses Arbeitskreises anerkannt zu werden, denn es wurde sich dafür entschieden, einen E-Mailverteiler zu führen, auf dem nur die Aufsichtsbehörden des Bundes und der Länder vertreten sind. Ebenso ist eine Mitarbeit an den Themen nicht erwünscht.

12 Ausblick und Schlussbemerkung

Die Herausforderungen im Datenschutz werden gewiss in den kommenden Jahren nicht geringer werden. Das Thema Künstliche Intelligenz wird noch mehr Fahrt aufnehmen, die damit zusammenhängenden rechtlichen Fragen sind weder einfach zu lösen noch trivial in ihren Auswirkungen. Und vor allem die politischen Entwicklungen in den Vereinigten Staaten von Amerika geben Anlass zur Sorge, ob ein Datentransfer mit den dortigen Anbietern weiterhin auf einer rechtlich stabilen Grundlage erfolgen kann. Dennoch sehe ich mit Zuversicht und Freude in die Zukunft.

Das hinter meinem Team und mir liegende Jahr war interessant, spannend und hat viel Neues bereitgehalten. Ich darf an dieser Stelle erneut betonen, dass die Zusammenarbeit in meiner Behörde in außerordentlich guter Weise funktioniert hat, das Engagement und die freundliche Atmosphäre sind bemerkenswert und nicht selbstverständlich. Daher spreche ich auch meinen Mitarbeitenden wiederholt meinen herzlichen Dank aus.

Die Aufsicht über insgesamt neun Rundfunkanstalten ist – wenig überraschend – eine fordernde Aufgabe. Es wäre wünschenswert, noch mehr Themen in den Blick zu nehmen, zusätzliche Befragungen und Audits durchzuführen und Orientierungshilfen und Handlungsempfehlungen in schneller Abfolge zu produzieren. Es ist nicht meine Art, ständig weitere Ressourcen anzumahnen, aber auch der Leistungsfähigkeit meiner Behörde sind an dieser Stelle Grenzen gesetzt. Zukünftig wird meinen Bereich sicherlich stark beeinflussen, ob der Reformstaatsvertrag in Kraft gesetzt wird und insofern die Aufsicht über alle Landesrundfunkanstalten einer Behörde zugeordnet wird. Dies hätte zur Folge, dass die Anzahl der Beschwerdeverfahren steigen wird und insgesamt ein höheres Arbeitsaufkommen zu erwarten ist. Dies wird Auswirkungen auf die Ausstattung der Datenschutz-Aufsicht haben müssen.

Ich bedanke mich bei allen Rundfunkanstalten, den Rundfunk, Fernseh- und Hörfunkräten, den Verwaltungsräten und ebenso den Geschäftsleitungen für die vertrauensvolle und stets gute und angenehme Zusammenarbeit. Ich habe zunehmend den Eindruck gewonnen, dass die Rolle, die der Aufsichtsbehörde im Gefüge des öffentlich-rechtlichen Rundfunks zukommt, wahr- und ernst genommen wird. Ich freue mich auf die vor mir liegenden Zeiten und blicke gespannt auf die Entwicklung des Datenschutzes im öffentlich-rechtlichen Rundfunk.

13 Anhang

13.1 DSGVO Art. 51 ff.

Artikel 51

Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird.

(2) Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union. Zu diesem Zweck arbeiten die Aufsichtsbehörden untereinander sowie mit der Kommission gemäß Kapitel VII zusammen.

(3) Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die diese Behörden im Ausschuss vertritt, und führt ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 63 einhalten.

(4) Jeder Mitgliedstaat teilt der Kommission bis spätestens 25. Mai 2018 die Rechtsvorschriften, die er aufgrund dieses Kapitels erlässt, sowie unverzüglich alle folgenden Änderungen dieser Vorschriften mit.

Artikel 52

Unabhängigkeit

(1) Jede Aufsichtsbehörde handelt bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse gemäß dieser Verordnung völlig unabhängig.

(2) Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Verordnung weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.

(3) Das Mitglied oder die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.

(4) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können.

(5) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde ihr eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der betreffenden Aufsichtsbehörde untersteht.

(6) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt und dass sie über eigene, öffentliche, jährliche Haushaltspläne verfügt, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

Artikel 55

Zuständigkeit

(1) Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.

(2) Erfolgt die Verarbeitung durch Behörden oder private Stellen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe c oder e, so ist die Aufsichtsbehörde des betroffenen Mitgliedstaats zuständig. In diesem Fall findet Artikel 56 keine Anwendung.

(3) Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

Artikel 57

Aufgaben

(1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

a) die Anwendung dieser Verordnung überwachen und durchsetzen;

b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;

c) im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten;

d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren;

e) auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeiten;

f) sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

g) mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;

h) Untersuchungen über die Anwendung dieser Verordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;

i) maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;

j) Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 und des Artikels 46 Absatz 2 Buchstabe d festlegen;

k) eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß Artikel 35 Absatz 4 eine Datenschutz-Folgenabschätzung durchzuführen ist;

l) Beratung in Bezug auf die in Artikel 36 Absatz 2 genannten Verarbeitungsvorgänge leisten;

m) die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Absatz 1 fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 bieten müssen, Stellungnahmen abgeben und sie billigen;

n) die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 billigen;

o) gegebenenfalls die nach Artikel 42 Absatz 7 erteilten Zertifizierungen regelmäßig überprüfen;

p) die Anforderungen an die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 abfassen und veröffentlichen;

q) die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 vornehmen;

r) Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 genehmigen;

s) verbindliche interne Vorschriften gemäß Artikel 47 genehmigen;

t) Beiträge zur Tätigkeit des Ausschusses leisten;

u) interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 ergriffene Maßnahmen und

v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

(2) Jede Aufsichtsbehörde erleichtert das Einreichen von in Absatz 1 Buchstabe f genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Die Erfüllung der Aufgaben jeder Aufsichtsbehörde ist für die betroffene Person und gegebenenfalls für den Datenschutzbeauftragten unentgeltlich.

(4) Bei offenkundig unbegründeten oder - insbesondere im Fall von häufiger Wiederholung - exzessiven Anfragen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

Artikel 58

Befugnisse

(1) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

a) den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,

b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,

c) eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen,

d) den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,

e) von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,

f) gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,

b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,

c) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,

d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen,

f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,

g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,

h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,

i) eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,

j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

(3) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Genehmigungsbefugnisse und beratenden Befugnisse, die es ihr gestatten,

a) gemäß dem Verfahren der vorherigen Konsultation nach Artikel 36 den Verantwortlichen zu beraten,

b) zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaats an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten,

c) die Verarbeitung gemäß Artikel 36 Absatz 5 zu genehmigen, falls im Recht des Mitgliedstaats eine derartige vorherige Genehmigung verlangt wird,

d) eine Stellungnahme abzugeben und Entwürfe von Verhaltensregeln gemäß Artikel 40 Absatz 5 zu billigen,

e) Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren,

f) im Einklang mit Artikel 42 Absatz 5 Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen,

g) Standarddatenschutzklauseln nach Artikel 28 Absatz 8 und Artikel 46 Absatz 2 Buchstabe d festzulegen,

h) Vertragsklauseln gemäß Artikel 46 Absatz 3 Buchstabe a zu genehmigen,

i) Verwaltungsvereinbarungen gemäß Artikel 46 Absatz 3 Buchstabe b zu genehmigen

j) verbindliche interne Vorschriften gemäß Artikel 47 zu genehmigen.

(4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.

(5) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen dieser Verordnung durchzusetzen.

(6) Jeder Mitgliedstaat kann durch Rechtsvorschriften vorsehen, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 2 und 3 aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. Die Ausübung dieser Befugnisse darf nicht die effektive Durchführung des Kapitels VII beeinträchtigen.

Artikel 59

Tätigkeitsbericht

Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen nach Artikel 58 Absatz 2 enthalten kann. Diese Berichte werden dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden übermittelt. Sie werden der Öffentlichkeit, der Kommission und dem Ausschuss zugänglich gemacht.

13.2 DSGVO Art. 85

Artikel 85

Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

(1) Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang.

(2) Für die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) vor, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

(3) Jeder Mitgliedstaat teilt der Kommission die Rechtsvorschriften, die er aufgrund von Absatz 2 erlassen hat, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften mit.

13.3 MStV § 12, § 23, § 113

§ 12

Datenverarbeitung zu journalistischen Zwecken, Medienprivileg

(1) Soweit die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio oder private Rundfunkveranstalter personenbezogene Daten zu journalistischen Zwecken verarbeiten, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen Zwecken von der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) außer den Kapiteln I, VIII, X und XI nur die Artikel 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Artikel 24 und Artikel 32 Anwendung.

Artikel 82 und 83 der Verordnung (EU) 2016/679 gelten mit der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses gemäß den Sätzen 1 bis 3 sowie für unzureichende Maßnahmen nach Artikel 5 Abs. 1 Buchst. f, Artikel 24und 32 der Verordnung (EU) 2016/679 gehaftet wird. Die Sätze 1 bis 5 gelten entsprechend für die zu den in Satz 1 genannten Stellen gehörenden Hilfs- und Beteiligungsunternehmen. Die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio und andere Rundfunkveranstalter sowie ihre Verbände und Vereinigungen können sich Verhaltenskodizes geben, die in einem transparenten Verfahren erlassen und veröffentlicht werden. Den betroffenen Personen stehen nur die in den Absätzen 2 und 3 genannten Rechte zu.

(2) Führt die journalistische Verarbeitung personenbezogener Daten zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, so sind diese Gegendarstellungen, Verpflichtungserklärungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

(3) Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, kann die betroffene Person Auskunft über die der Berichterstattung zugrundeliegenden, zu ihrer Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen mitwirken oder mitgewirkt haben, geschlossen werden kann,

2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann oder

3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde. Die betroffene Person kann die unverzügliche Berichtigung unrichtiger personenbezogener Daten im Datensatz oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Die weitere Speicherung der personenbezogenen Daten ist rechtmäßig,

wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Wahrnehmung berechtigter Interessen erforderlich ist.

(4) Für die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio und private Rundfunkveranstalter sowie zu diesen gehörende Beteiligungs- und Hilfsunternehmen wird die Aufsicht über die Einhaltung der geltenden datenschutzrechtlichen Bestimmungen durch Landesrecht bestimmt. Regelungen dieses Staatsvertrages bleiben unberührt.

(5) Die Absätze 1 bis 4 gelten auch für Teleshoppingkanäle.

---

§ 23

Datenverarbeitung zu journalistischen Zwecken, Medienprivileg

(1) Soweit die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio, private Rundfunkveranstalter oder Unternehmen und Hilfsunternehmen der Presse als Anbieter von Telemedien personenbezogene Daten zu journalistischen Zwecken verarbeiten, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen Zwecken außer den Kapiteln I, VIII, X und XI der Verordnung (EU) 2016/679 nur die Artikel 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Artikel 24 und Artikel 32 der Verordnung (EU) 2016/679 Anwendung. Artikel 82 und 83 der Verordnung (EU) 2016/679 gelten mit der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses gemäß den Sätzen 1 bis 3 sowie für unzureichende Maßnahmen nach Artikel 5 Abs. 1 Buchst. f, Artikel 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird. Kapitel VIII der Verordnung (EU) 2016/679 findet keine Anwendung, soweit Unternehmen, Hilfs- und Beteiligungsunternehmen der Presse der Selbstregulierung durch den Pressekodex und der Beschwerdeordnung des Deutschen Presserates unterliegen. Die Sätze 1 bis 6 gelten entsprechend für die zu den in Satz 1 genannten Stellen gehörenden Hilfs- und Beteiligungsunternehmen. Den betroffenen Personen stehen nur die in den Absätzen 2 und 3 genannten Rechte zu.

(2) Werden personenbezogene Daten von einem Anbieter von Telemedien zu journalistischen Zwecken gespeichert, verändert, übermittelt, gesperrt oder gelöscht und wird die betroffene Person dadurch in ihrem Persönlichkeitsrecht beeinträchtigt, kann sie Auskunft über die zugrundeliegenden, zu ihrer Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung mitgewirkt haben, geschlossen werden kann,

2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann oder 3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe des Anbieters durch Ausforschung des Informationsbestandes beeinträchtigt würde. Die betroffene Person kann die unverzügliche Berichtigung unrichtiger personenbezogener Daten im Datensatz oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Die weitere Speicherung der personenbezogenen Daten ist rechtmäßig, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Wahrnehmung berechtigter Interessen

erforderlich ist. Die Sätze 1 bis 3 gelten nicht für Angebote von Unternehmen, Hilfs- und Beteiligungsunternehmen der Presse, soweit diese der Selbstregulierung durch den Pressekodex und der Beschwerdeordnung des Deutschen Presserates unterliegen. (3) Führt die journalistische Verarbeitung personenbezogener Daten zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, sind diese Gegendarstellungen, Verpflichtungserklärungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

---

§ 113

Datenschutzaufsicht bei Telemedien

Die nach den allgemeinen Datenschutzgesetzen des Bundes und der Länder zuständigen Aufsichtsbehörden überwachen für ihren Bereich die Einhaltung der allgemeinen Datenschutzbestimmungen und des § 23. Die für den Datenschutz im journalistischen Bereich beim öffentlich-rechtlichen Rundfunk und bei den privaten Rundfunkveranstaltern zuständigen Stellen überwachen für ihren Bereich auch die Einhaltung der Datenschutzbestimmungen für journalistisch redaktionell-gestaltete Angebote bei Telemedien. Eine Aufsicht erfolgt, soweit Unternehmen, Hilfs- und Beteiligungsunternehmen der Presse nicht der Selbstregulierung durch den Pressekodex und der Beschwerdeordnung des Deutschen Presserates unterliegen.

13.4 TDDDG § 25

§ 25 TDDDG

Schutz der Privatsphäre bei Endeinrichtungen

(1) Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 679/2016 zu erfolgen.

(2) Die Einwilligung nach Absatz 1 ist nicht erforderlich,

1. wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder

2. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines digitalen Dienstes einen vom Nutzer ausdrücklich gewünschten digitalen Dienst zur Verfügung stellen kann.

13.5 Regelungen zum Rundfunkdatenschutzbeauftragten

Darstellung der Regelungen am Beispiel des MDR-Staatsvertrages:

§ 38

Ernennung der Rundfunkbeauftragten oder des Rundfunkbeauftragten für den Datenschutz beim MDR und der Datenschutzbeauftragten oder des Datenschutzbeauftragten des MDR

(1) Der MDR ernennt eine Rundfunkbeauftragte oder einen Rundfunkbeauftragten für den Datenschutz beim MDR (Rundfunkdatenschutzbeauftragte oder Rundfunkdatenschutzbeauftragter), der zuständige Aufsichtsbehörde im Sinne des Artikels 51 der Verordnung (EU) 2016/679 ist. Die Ernennung erfolgt durch den Rundfunkrat mit Zustimmung des Verwaltungsrates für die Dauer von vier Jahren. Eine dreimalige Wiederernennung ist zulässig. Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, nachgewiesen durch ein abgeschlossenes Hochschulstudium, sowie über Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Das Amt der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten kann nicht neben anderen Aufgaben innerhalb des MDR und seiner Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten zu vereinbaren sein und dürfen ihre oder seine Unabhängigkeit nicht gefährden.

(2) Das Amt endet mit Ablauf der Amtszeit, mit Rücktritt vom Amt oder mit Erreichen des gesetzlichen Renteneintrittsalters. Tarifvertragliche Regelungen bleiben unberührt. Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte kann ihres oder seines Amtes nur enthoben werden, wenn sie oder er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Dies geschieht durch Beschluss des Rundfunkrates auf Vorschlag des Verwaltungsrates; die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte ist vor der Entscheidung zu hören.

(3) Das Nähere, insbesondere die Grundsätze der Vergütung, beschließt der Rundfunkrat mit Zustimmung des Verwaltungsrates in einer Satzung.

(4) Die Datenschutzbeauftragte oder der Datenschutzbeauftragte des MDR nach Artikel 37 der Verordnung (EU) 2016/679 wird von der Intendantin oder von dem Intendanten mit Zustimmung des Verwaltungsrates benannt.

---

§ 39

Unabhängigkeit der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten

(1) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte ist in Ausübung ihres oder seines Amtes unabhängig und nur dem Gesetz unterworfen. Sie oder er unterliegt keiner Rechts- oder Fachaufsicht. Der Dienstaufsicht des Verwaltungsrates untersteht sie oder er nur insoweit, als ihre oder seine Unabhängigkeit bei der

Ausübung ihres oder seines Amtes dadurch nicht beeinträchtigt wird. (2) Die Dienststelle der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten wird bei der Geschäftsstelle von Rundfunkrat und Verwaltungsrat eingerichtet. Der Rundfunkdatenschutzbeauftragten oder dem Rundfunkdatenschutzbeauftragten ist die für die Erfüllung ihrer oder seiner Aufgaben und Befugnisse notwendige Personal-, Finanz- und Sachausstattung zur Verfügung zu stellen. Die erforderlichen Mittel sind jährlich, öffentlich und gesondert im Haushaltsplan des MDR auszuweisen und der Rundfunkdatenschutzbeauftragten oder dem Rundfunkdatenschutzbeauftragten im Haushaltsvollzug zuzuweisen. Einer Finanzkontrolle durch den Verwaltungsrat unterliegt die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte nur insoweit, als ihre oder seine Unabhängigkeit bei der Ausübung ihres oder seines Amtes dadurch nicht beeinträchtigt wird. (3) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte ist in der Wahl ihrer Mitarbeiterinnen oder seiner Mitarbeiter frei. Sie unterstehen allein ihrer oder seiner Leitung.

---

§ 40

Aufgaben und Befugnisse der Rundfunkdatenschutzbeauftragen oder des Rundfunkdatenschutzbeauftragten

(1) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Datenschutzvorschriften dieses Staatsvertrages, des MStV, der Verordnung (EU) 2016/679 und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des MDR und seiner Beteiligungsunternehmen im Sinne des § 42 Absatz 3 Satz 1 MStV. Sie oder er hat die Aufgaben und Befugnisse entsprechend der Artikel 57 und 58 Absatz 1 bis 5 der Verordnung (EU) 2016/679. Bei der Zusammenarbeit mit anderen Aufsichtsbehörden hat sie oder er, soweit die Datenverarbeitung zu journalistischen Zwecken betroffen ist, den Schutz von Informanten zu wahren. Sie oder er kann gegenüber dem MDR keine Geldbußen verhängen.

(2) Stellt die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte Verstöße gegen Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet sie oder er dies gegenüber der Intendantin oder dem Intendanten und fordert sie oder ihn zur Stellungnahme innerhalb einer angemessenen Frist auf. Gleichzeitig unterrichtet sie oder er den Verwaltungsrat. Von einer Beanstandung und Unterrichtung kann abgesehen werden, wenn es sich um unerhebliche Mängel handelt oder wenn ihre unverzügliche Behebung sichergestellt ist.

(3) Die von der Intendantin oder von dem Intendanten nach Absatz 2 Satz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der Rundfunkdatenschutzdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten getroffen worden sind. Die Intendantin oder der Intendant leitet dem Verwaltungsrat gleichzeitig eine Abschrift der Stellungnahme gegenüber der Rundfunkdatenschutzbeauftragten oder dem Rundfunkdatenschutzbeauftragten zu.

(4) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte erstattet jährlich auch den Organen des MDR den schriftlichen Bericht im Sinne des Artikels 59 der Verordnung (EU) 2016/679 über ihre oder seine Tätigkeit. Der Bericht wird veröffentlicht, wobei eine Veröffentlichung im Online-Angebot des MDR ausreichend ist.

(5) Jeder hat das Recht, sich unmittelbar an die Rundfunkdatenschutzbeauftragte oder den Rundfunkdatenschutzbeauftragten zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen

Daten durch den MDR oder seinen Beteiligungsunternehmen im Sinne des Absatzes 1 Satz 1 in seinen schutzwürdigen Belangen verletzt zu sein.

(6) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte ist sowohl während als auch nach Beendigung ihrer oder seiner Tätigkeit verpflichtet, über die ihr oder ihm während ihrer oder seiner Dienstzeit bekanntgewordenen Angelegenheiten und vertraulichen Informationen Verschwiegenheit zu bewahren.

13.6 RDSK-Mitgliederliste

Rundfunkdatenschutzbeauftragte/r	Rundfunkanstalt/en
Stephan Schwarze	BR - Bayerischer Rundfunk HR - Hessischer Rundfunk MDR - Mitteldeutscher Rundfunk rbb - Radio Berlin-Brandenburg SR - Saarländischer Rundfunk SWR - Südwestrundfunk WDR - Westdeutscher Rundfunk DRadio - Deutschlandradio ZDF - Zweites Deutsches Fernsehen
Thomas Gardemann	DW - Deutsche Welle
Dr. Heiko Neuhoff	NDR - Norddeutscher Rundfunk
Ivka Jurčević	RB - Radio Bremen

13.7 RDSK-Verwaltungsvereinbarung

Verwaltungsvereinbarung
zur Wahrnehmung der Datenschutzaufsicht
über Gemeinschaftseinrichtungen und Gemeinschaftsunternehmen
der Rundfunkanstalten
vom 01.12.2023

Der Rundfunkdatenschutzbeauftragte beim Bayerischen Rundfunk, Hessischen Rundfunk, Mitteldeutschen Rundfunk, Rundfunk Berlin-Brandenburg, Saarländischen Rundfunk, Südwestrundfunk, Westdeutschen Rundfunk, Deutschlandradio und Zweiten Deutschen Fernsehen,

der Rundfunkdatenschutzbeauftragte beim Norddeutschen Rundfunk,

die Beauftragte für den Datenschutz bei Radio Bremen,

und

der Beauftragte für den Datenschutz der Deutschen Welle

(im Folgenden: Aufsichtsbehörden) schließen zur Wahrnehmung der Datenschutzaufsicht über die Gemeinschaftseinrichtungen der Rundfunkanstalten und über Unternehmen, an denen die von ihnen zu beaufsichtigenden Rundfunkanstalten insgesamt oder teilweise unmittelbar oder mittelbar gemeinschaftlich beteiligt sind (Gemeinschaftsunternehmen), folgende Vereinbarung:

§ 1 Federführung

(1) Die Aufsicht über jede Gemeinschaftseinrichtung und jedes Gemeinschaftsunternehmen nimmt eine Aufsichtsbehörde federführend wahr. Ihre Handlungen und Erklärungen wirken im Verhältnis zu den für die Gemeinschaftseinrichtung Verantwortlichen oder zum Gemeinschaftsunternehmen für und gegen die anderen Aufsichtsbehörden.

(2) Die Federführungen und die jeweils beteiligten Aufsichtsbehörden ergeben sich aus der als Anlage beigefügte Übersicht.

(3) Die Aufgaben und Befugnisse jeder beteiligten Aufsichtsbehörde nach den Artt. 57 f. DSGVO bzw. den jeweils maßgeblichen gesetzlichen Vorschriften bleiben von einer Federführung unberührt.

1

§ 2 Zuständigkeit der federführenden Aufsichtsbehörde

(1) Die federführende Aufsichtsbehörde ist zuständig für die Entgegennahme und Bearbeitung von Meldungen nach Art. 33 DSGVO.

(2) Die federführende Aufsichtsbehörde nimmt im Verhältnis zu den für die jeweilige Gemeinschaftseinrichtung Verantwortlichen sowie zum jeweiligen Gemeinschaftsunternehmen die Aufgaben und Befugnisse wahr, die sich aus der DSGVO bzw. den jeweils maßgeblichen gesetzlichen Vorschriften ergeben.

(3) Die federführende Aufsichtsbehörde ist primärer Ansprechpartner für die oder den jeweilige/n Datenschutzbeauftragte/n der Gemeinschaftseinrichtung/des Gemeinschaftsunternehmens nach Art. 37 DSGVO.

§ 3 Abstimmung zwischen dem Federführer und den anderen Aufsichtsbehörden

(1) Soweit nachfolgend nicht anderweitig geregelt, nimmt der jeweilige Federführer die Aufgaben der Aufsicht eigenständig wahr. Die anderen beteiligten Aufsichtsbehörden sind berechtigt, vom Federführer jederzeit Auskunft über etwaige Empfehlungen, aufsichtsrechtliche Verfahren oder Maßnahmen zu verlangen oder ihn zu solchen Verfahren oder Maßnahmen aufzufordern.

(2) Der Federführer informiert die anderen beteiligten Aufsichtsbehörden vorab über eine Empfehlung bzw. Maßnahme im Rahmen einer vorherigen Konsultation nach Art. 36 DSGVO, eine Datenschutzüberprüfung nach Art. 58 Abs. 1 lit. b) DSGVO oder die Verhängung einer Geldbuße nach Art. 58 Abs. 2 lit. i) DSGVO und gibt ihnen Gelegenheit zur Stellungnahme innerhalb einer Frist von mindestens drei Wochen. Beabsichtigt der Federführer, sich einem innerhalb dieser Frist eingegangenen Änderungswunsch anzuschließen, legt er den beteiligten Aufsichtsbehörden einen überarbeiteten Entwurf vor und gibt ihnen Gelegenheit zur erneuten Stellungnahme innerhalb von 12 Werktagen. Sofern innerhalb dieser Frist ein weiterer Widerspruch eingeht, wiederholt er das Verfahren nach Satz 1 und 2. An eine auf dieser Grundlage vorgenommene aufsichtsrechtliche Handlung des Federführers sind die beteiligten Aufsichtsbehörden gebunden.

(3) Das Recht jeder beteiligten Aufsichtsbehörde, sich an einer vom Federführer beabsichtigen Datenschutzüberprüfung nach Art. 58 Abs. 2 lit. i) DSGVO zu beteiligen, bleibt hiervon unberührt.

(4) Der Federführer stellt jeder beteiligten Aufsichtsbehörde auf Wunsch alle relevanten Informationen und Daten zur Aufsicht über die betreffende Gemeinschaftseinrichtung oder das betreffende Gemeinschaftsunternehmen für ihren jeweiligen Tätigkeitsbericht oder sonstige Anlässe zur Verfügung.

§ 4 Informationsaustausch

Der Federführer und die anderen beteiligten Aufsichtsbehörden tauschen untereinander alle zweckdienlichen Informationen zur Aufsicht über die jeweilige Gemeinschaftseinrichtung oder das jeweilige Beteiligungsunternehmen aus.

§ 5 Geltungsdauer, Kündigung

(1) Die Vereinbarung tritt am 1. Januar 2024 in Kraft und gilt zunächst bis zum 31. Dezember 2026. Sie verlängert sich um jeweils ein weiteres Jahr, sofern nicht eine der Vertragsparteien spätestens zum 30. September eines Kalenderjahres kündigt.

(2) Die Kündigung kann schriftlich oder per E-Mail erklärt und muss allen Vertragspartnern zugestellt werden. Für die Wirksamkeit der Kündigung genügt der fristgemäße Eingang bei einem der Vertragspartner.

(3) Diese Veraltungsvereinbarung ersetzt die Verwaltungsvereinbarungen (1) zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten vom 29. Juli 2020
und (2) zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten vom 29. Juli 2020.

§ 6 Sonstiges

(1) Mündliche Nebenabreden sind unwirksam. Jede Änderung dieser Vereinbarung einschließlich dieser Vorschrift bedarf der Schriftform und des Einvernehmens aller Vertragsparteien.

(2) Änderungen der Anlage lassen die Geltung der Verwaltungsvereinbarung unberührt. Im Übrigen gilt Absatz 1 entsprechend.

Anlage:
Gemeinschaftseinrichtungen und Gemeinschaftsunternehmen, Federführung

Leipzig, den

Der Rundfunkdatenschutzbeauftragte beim BR, HR, MDR, rbb, SR, SWR, WDR, DRadio und ZDF

Hamburg, den

Der Rundfunkdatenschutzbeauftragte beim NDR

Bremen, den

Die Beauftragte für den Datenschutz bei Radio Bremen

Bonn, den

Der Beauftragte für den Datenschutz der Deutschen Welle

4

Anlage zur
Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht
über Gemeinschaftseinrichtungen und über Gemeinschaftsunternehmen der Rundfunkanstalten
Stand: Mai 2024

	Beteiligte Rundfunkanstalten (Federführung)	Federführendes RDSK-Mitglied	GSEA oder Beteiligungs-unternehmen
Archivprozesse ZEMI	Alle LRF (BR)	RDSB BR	GSEA
ARD aktuell inkl. tagesschau.de	Alle LRF (NDR)	RDSB NDR	GSEA
ARD Channels International (vormals Kabelkoordination Ausland)	Alle LRF (WDR)	RDSB WDR	GSEA
ARD/Deutschlandradio Steuerbüro	Alle LFR (SWR)	RDSB SWR	GSEA
ARD Generalsekretariat	Alle LFR (rbb/gf Anstalt)	DSB rbb	GSEA
ARD Hauptstadtstudio	Alle LFR (rbb/WDR)	DSB rbb	GSEA
ARD-Hörfunk-Korrespondentennetz in Zusammenarbeit mit DRadio	Alle LFR (WDR)	RDSB WDR	GSEA
ARD Kultur	Alle LFR (MDR)	RDSB MDR	GSEA
ARD Media GmbH, Frankfurt/M	BR, MDR, NDR, SR, SWR, WDR (SR)	RDSB SR	Beteiligungsunternehmen
ARD Online	Alle LFR (SWR)	RDSB SWR	GSEA
ARD-Partnermanagement Audio und Voice	Alle LFR (WDR)	RDSB WDR	GSEA
ARD Play-Out-Center	Alle LFR (rbb)	DSB rbb	GSEA
ARD-Programmdirektion inkl. DasErste.de	Alle LFR (BR)	RDSB BR	GSEA
ARD-Sportschau-Redaktion	Alle LFR (WDR)	RDSB WDR	GSEA
ARD Sternpunkt	Alle LFR (HR)	DSB HR	GSEA
ARD Text	Alle LFR (rbb)	DSB rbb	GSEA
ARD-TV-Leitungsbüro	Alle LFR + DW (NDR)	RDSB NDR	GSEA
ARGE Rundfunk-Betriebstechnik	Alle LFR (BR)	RDSB BR	GSEA
ARD ZDF Deutschlandradio Beitragsservice	Alle LFR, DRadio, ZDF (WDR)	Beitragszahlende: Jew. RDSB von BR, MDR, NDR, rbb, SR, SWR, WDR Im Übrigen: RDSB WDR	GSEA
ARD.ZDF medienakademie gGmbH, Nürnberg	BR, MDR, NDR, SR, SWR, WDR, DW, DRadio, ZDF (BR)	RDSB BR	Beteiligungsunternehmen
ARTE Deutschland TV GmbH, Baden-Baden	BR, MDR, NDR, SR, SWR, WDR, ZDF (SWR)	RDSB SWR	Beteiligungsunternehmen
AS&S Radio GmbH, Frankfurt/M	BR, MDR, NDR, SR, SWR, WDR (SR)	RDSB SR	Beteiligungsunternehmen
Baden-Badener Pensionskasse VVaG, Baden-Baden	BR, MDR, NDR, SR, SWR, WDR, DRadio (SWR)	RDSB SWR	Beteiligungsunternehmen
Bavaria Film GmbH, München	BR, MDR, SWR, WDR (BR)	RDSB BR	Beteiligungsunternehmen
Beteiligung der ARD an 3sat	ZDF, alle LFR (ZDF)	RDSB ZDF	GSEA
DEGETO Film GmbH, Frankfurt/M	BR, MDR, NDR, SR, SWR, WDR (NDR)	RDSB NDR	Beteiligungsunternehmen
Deutsches Rundfunkarchiv (DRA), Frankfurt/M	BR, MDR, NDR, SR, SWR, WDR, DRadio, DW (DRadio)	RDSB DRadio	Beteiligungsunternehmen

Ereignis- und Dokumentationskanal Phoenix	Alle LFR, ZDF (ZDF/WDR)	RDSB ZDF	GSEA
EU-Verbindungsbüro in Brüssel	Alle LFR (WDR)	RDSB WDR	GSEA
Finanzmarktberichterstattung	Alle LFR (HR)	RDSB HR	GSEA
Funk (Junges Angebot von ARD & ZDF)	Alle LFR. ZDF (SWR)	RDSB SWR	GSEA
Geschäftsstelle der ARD-Gremienvorsitzendenkonferenz	Alle LFR (BR)	RDSB BR	GSEA
Informations-Verarbeitungs-Zentrum IVZ	Mitglieder ARD, DRadio (rbb)	DSB rbb	GSEA
Innovations- und Digitalagentur (ida) GmbH	MDR, ZDF (MDR)	RDSB MDR	Beteiligungsunternehmen
KEF-Büro der ARD	Alle LFR (NDR)	RDSB NDR	GSEA
KiKA - Der Kinderkanal von ARD & ZDF	Alle LFR, ZDF (MDR)	RDSB MDR	GSEA
One	Alle LFR (WDR)	RDSB WDR	GSEA
Pensionskasse Rundfunk VVaG, Frankfurt/M	BR, MDR, NDR, SR, SWR, WDR (WDR)	RDSB WDR	Beteiligungsunternehmen
Saxonia Media Filmproduktionsgesellschaft mbH, Leipzig	BR, MDR (MDR)	RDSB MDR	Beteiligungsunternehmen
SportA GmbH, München	BR, MDR, NDR, SR, SWR, WDR, ZDF (ZDF)	RDSB ZDF	Beteiligungsunternehmen
Sportschau.de	Alle LFR (WDR)	RDSB WDR	GSEA
Stiftung Zuhören, Gießen/München	BR, MDR, NDR, SR (BR)	RDSB BR	Beteiligungsunternehmen
Tagesschau24	Alle LFR (NDR)	RDSB NDR	GSEA
Zentrale Schallplattenkatalogisierung (ZSK)	Alle LFR (HR)	RDSB HR	GSEA