Landtag von Baden-Württemberg **Drucksache 17 / 6813**

17. Wahlperiode **4.4.2024**

Mitteilung

des Rundfunkdatenschutzbeauftragten

Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten für den Zeitraum 1. Januar 2023 bis 31. Dezember 2023

Schreiben des Rundfunkdatenschutzbeauftragten vom 4. April 2024:

Zu meinen Aufgaben als Rundfunkdatenschutzbeauftragter u. a. beim Südwestrundfunk und damit unabhängige Aufsichtsbehörde im Sinne von Artikel 51 EU Datenschutz-Grundverordnung (DSGVO) gehört die Überwachung der Einhaltung der Datenschutzvorschriften bei der gesamten Tätigkeit des Südwestrundfunks und seiner Beteiligungsunternehmen.

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. Davon ausgehend übersende ich Ihnen als Anlage meinen Tätigkeitsbericht des Jahres 2023 mit der höflichen Bitte um Kenntnisnahme.

Schwarze

Eingegangen: 4.4.2024 / Ausgegeben: 24.5.2024

BR hr mdr rbb SR SWR WDR ZDF Deutschlandradio

TÄTIGKEITS BERICHT

des Rundfunkdatenschutzbeauftragten

23

Der Rundfunkdatenschutzbeauftragte

Stephan Schwarze

Kantstraße 71-73, 04275 Leipzig

www.rundfunkdatenschutz.de

Leipzig, März 2024

Berichtszeitraum: 01.01.2023 bis 31.12.2023

Inhaltsverzeichnis

Vorwort

Nachdem ich bereits im Jahr 2022 die Aufsicht über den Südwestrundfunk übernommen hatte, kamen im Jahr 2023 der Bayerische Rundfunk, der Hessische Rundfunk, der Saarländische Rundfunk, der Westdeutsche Rundfunk, Deutschlandradio und das ZDF hinzu. Im Sommer des Berichtsjahres hat sich auch der Rundfunk Berlin-Brandenburg entschlossen, der gemeinsamen Aufsicht beizutreten.

Mit diesem Bericht verfolge ich die Absicht, einen Überblick über mein erstes Jahr als Rundfunkdatenschutzbeauftragter und damit Datenschutz - Aufsichtsbehörde bei insgesamt neun Rundfunkanstalten[1] zu geben. Aufgrund dieser nunmehr stattlichen Anzahl wird dieser Bericht ein wenig anders als meine bisherigen aufgebaut sein. Es wird verstärkt um Datenschutzgrundsätze und allgemeine Themen gehen, die mich und die Aufsichtsbehörde insgesamt - auch im Hinblick auf die Vergrößerung - umgetrieben und beschäftigt haben.

Das Jahr war geprägt vom Aufbau dieses Bereichs und der „Sortierung“ der Themen. Neben der erforderlichen Schwerpunktsetzung war das Jahr gefüllt mit Terminen, da es erforderlich und auch mein Wunsch war, mich in den Rundfunkanstalten vorzustellen. Dort habe ich verschiedene Themen angerissen und auch sehr deutlich darauf hingewiesen, dass die Verantwortung für die Umsetzung der datenschutzrechtlichen Anforderungen im Schwerpunkt bei den Rundfunkanstalten selbst und nicht bei den internen oder betrieblichen Datenschutzbeauftragten liegt (siehe dazu Kapitel 2.2 Vorstellung in den Direktorien). Insgesamt habe ich ein sehr positives Feedback erfahren, musste aber auch der Annahme entgegentreten, dass ich als (Aufsichts-)Rundfunkdatenschutzbeauftragter mit allen Datenschutz-Themen in den Rundfunkanstalten im Detail vertraut und damit auskunftsfähig bin. Meine Rolle ist dahingehend zu verstehen, dass ich die Schwerpunkte für meine Arbeit in eigener Verantwortung setze, dessen ungeachtet aber für Sachverhalte oder Probleme, die aus den Rundfunkanstalten an mich herangetragen werden, offen und jederzeit bereit bin, mit Rat und Tat zur Seite zu stehen und mich auch für übergeordnete Themen zu engagieren. Dies ist ein hoher Anspruch, es wird sich in den nächsten Jahren erweisen, ob dies in der von mir intendierten Form umgesetzt werden kann.

Mich würde es freuen, wenn es gelänge, in meinen Berichten einen grundsätzlichen und aussagekräftigen Überblick über die Datenschutzrealitäten in den Rundfunkanstalten zu geben. Dies hängt natürlich auch von den mir zur Verfügung stehenden Ressourcen ab, ich bin aber zuversichtlich.

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

Im Berichtsjahr konnte ich ab Mai auf die Unterstützung eines juristischen Referenten zurückgreifen, und auch mein Büro wurde in der bewährten Form gemanagt. Herrn Constantin Rechenberg und Frau Kirsten Schmidt danke ich ausdrücklich und sehr herzlich für ihre tatkräftige Unterstützung und ihr großes Engagement. Ohne dieses wäre der vorliegende Bericht nicht in der Form zu gestalten gewesen. Im Jahr 2024 kann ich überdies auf die Unterstützung einer weiteren Referentin zurückgreifen, die mich insbesondere in den Fragen der Datensicherheit und Informationstechnik unterstützen wird. An dieser Stelle danke ich ebenso Frau Susanne Wetterling, die an diesem Bericht im Hinblick auf die Gestaltung maßgeblich mitgewirkt hat.

Ich blicke auf ein ereignisreiches und in Teilen auch turbulentes Jahr zurück und kann als Fazit und als Resümee ziehen, dass Vieles gut gelungen ist und ebenso Vieles noch intensiver bearbeitet werden könnte. Ich kann bestätigen, dass die Konstruktion eines gemeinsamen Rundfunkdatenschutzbeauftragten über nunmehr neun Rundfunkanstalten funktioniert und ein tragfähiges Konzept darstellt. Schon an verschiedenen Stellen habe ich allerdings auch den Anspruch formuliert, dass der Rundfunkdatenschutzbeauftragte institutionalisiert und als gemeinsame Aufsicht über die Rundfunkanstalten staatsvertraglich festgeschrieben werden sollte. Dies ist ein Ziel, das ich gemeinsam mit den politisch Verantwortlichen zu verfolgen beabsichtige und bin gespannt auf die weiteren Entwicklungen.

Nun wünsche ich der interessierten Leserin und ebenso dem interessierten Leser eine Lektüre, die dem oben formulierten Anspruch gerecht wird, und auch dem „datenschutzrechtlichen Laien“ verständliche und nachvollziehbare Einblicke in meine Tätigkeit ermöglicht.

Leipzig, im März 2024
Stephan Schwarze

1 Einleitung

Mit diesem Tätigkeitsbericht komme ich meiner Pflicht aus Artikel 59 DSGVO nach, einen Bericht über meine Tätigkeit vorzulegen. Die für die gemeinsame Aufsicht über insgesamt neun Rundfunkanstalten maßgeblichen Vorschriften sehen vor, dass ich diesen Bericht den Organen zur Verfügung zu stellen habe. Dies sind die Verwaltungsräte, die Rundfunk-, Hörfunk- oder Fernsehräte sowie die Intendantinnen und Intendanten, die ich förmlich über meinen Bericht unterrichte. Ebenso habe ich diesen Bericht zu veröffentlichen, was ich auf meiner Website www.rundfunkdatenschutz.de tun werde. 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.

Das Berichtsjahr war geprägt vom Aufbau und der Erweiterung der bereits bestehenden Behörde. Durch den Aufgaben- und Verantwortungszuwachs war ich einerseits vor die Herausforderung gestellt, meine Aufsicht so zu gestalten, dass ich den gesetzlichen Verpflichtungen nachkomme, andererseits aber auch die richtige und angemessene Auswahl der von mir verfolgten Aktivitäten zu treffen, damit ein effektiver Datenschutz in aufsichtsrechtlicher Hinsicht gewährleistet wird. Dies - so gestehe ich freimütig - war nicht immer einfach und hat mich gefordert. Hilfreich war in diesem Zusammenhang, dass es gelungen ist, einen juristischen Referenten zu verpflichten, der sich in kürzester Zeit in die Themen und datenschutzrechtlichen Problematiken eingearbeitet hat.

Zuvorderst musste das von meinem Amtsvorgänger genutzte Dokumentenmanagementsystem in die Systeme meines Bereichs integriert werden, was einige technische und organisatorische Herausforderungen mit sich gebracht hat. Nach den zu erwartenden Startschwierigkeiten ist dieses Unterfangen geglückt, sodass die kontinuierliche Sacharbeit gewährleistet werden konnte. Die notwendigen Abstimmungen mit dem für die infrastrukturelle Ausstattung verantwortlichen Mitteldeutschen Rundfunk sind reibungslos verlaufen, dieser stellt gemäß der Verwaltungsvereinbarung zum gemeinsamen Rundfunkdatenschutzbeauftragten die administrativen und technischen Ressourcen zur Verfügung. Ich darf mich an dieser Stelle beim MDR und bei den befassten Mitarbeiterinnen und Mitarbeitern für das große Engagement und das stets offene Ohr für meine Sorgen und Nöte bedanken.

Im ersten Jahr meiner gemeinsamen Aufsichtszuständigkeit habe ich es als meine Pflicht angesehen, mir einerseits einen Überblick zu verschaffen und andererseits wichtige Themen voranzutreiben, dies gemeinsam und in Zusammenarbeit mit den anderen Rundfunkdatenschutzbeauftragten des Norddeutschen Rundfunks, des Rundfunks Berlin-Brandenburg (bis zum 30.06.2023), von Radio Bremen und der Deutschen Welle.

Das vielleicht spannendste Thema im abgelaufenen Jahr war die geradezu explosionsartig zugenommene Bedeutung von Künstlicher Intelligenz, deren neue Anwendungsformen in einer

scheinbar plötzlichen Art und Weise zum allgegenwärtigen Thema geworden sind. Die Rundfunkdatenschutzkonferenz hat unter meiner maßgeblichen Mitwirkung einen ersten Problemaufriss zu diesem Thema erstellt und Handlungsanweisungen für den öffentlich-rechtlichen Rundfunk skizziert. Ich habe die Hoffnung, dass diese Orientierungshilfe tauglich und geeignet ist, im doch recht schwierigen Umfeld von Künstlicher Intelligenz datenschutzrechtliche Leitplanken sichtbar zu machen. Dazu finden sich im Bericht unter Kapitel 6.2 noch vertiefende Informationen.

1.1 Änderung des Staatsvertrags über den rbb

Zum 01.07.2023 habe ich auch die Aufsicht über den Rundfunk Berlin-Brandenburg (rbb) übernommen. Der rbb gehörte bisher zu den Rundfunkanstalten, die einer sogenannten geteilten Aufsicht unterlagen. Dies bedeutet, dass die/der Rundfunkdatenschutzbeauftragte sich nur um die Datenverarbeitung mit journalistischem Kontext zu kümmern hatte und demgegenüber die staatlichen Aufsichten des Sendegebietes der betreffenden Rundfunkanstalt über die restlichen sogenannten Verwaltungsdaten wachten. Unabhängig davon, dass die Abgrenzung relativ schwierig ist und sich nicht zuletzt deshalb die Aufsicht der staatlichen Behörden hauptsächlich auf die Datenverarbeitung im Zusammenhang mit der Rundfunkbeitragserhebung beschränkte, hat dieses System seit jeher auch verfassungsrechtliche Fragen aufgeworfen. Es verträgt sich nach einhelliger Auffassung des Rundfunks nur begrenzt mit der Staatsferne desselben, dass staatliche Aufsichtsbehörden Einfluss auf Bereiche der Rundfunkanstalten ausüben. Insofern ist es sehr zu begrüßen, dass sich mit Verabschiedung des neuen Staatsvertrags der rbb mit dem 01.01.2024 auch in die Reihe derer einreihen kann, die vollständig der Aufsicht eines Rundfunkdatenschutzbeauftragten unterliegen. Folglich ist die Frage nicht mehr beachtlich, wie die unterschiedlichen Datenkategorien - redaktionelle oder journalistische Daten einerseits und sonstige Verwaltungsdaten andererseits - voneinander abzugrenzen sind.

Im Rahmen meiner Vorstellung in der rbb Geschäftsleitung habe ich diese Neuerung erläutert und die Aufgaben des Rundfunkdatenschutzbeauftragten erklärt. Insbesondere hatte ich darauf hingewiesen, dass der Rundfunkdatenschutzbeauftragte nicht sämtliche Datenverarbeitungen des rbb in den Blick zu nehmen hat, sondern als Aufsicht nach eigenem Ermessen über bestimmte datenschutzrechtliche Themen - auch in Ansehung der gemeinsamen Aufsicht über insgesamt neun Rundfunkanstalten - befinden kann. Insofern freue ich mich nunmehr auf die „ungeteilte Aufmerksamkeit“, die ich dem rbb zuteilwerden lassen kann.

1.2 Verwaltungsvereinbarung gemeinsamer Rundfunkdatenschutzbeauftragter

Schon frühzeitig war klar, dass die Konstruktion eines gemeinsamen Rundfunkdatenschutzbeauftragten für jetzt insgesamt sieben Landesrundfunkanstalten, das ZDF sowie Deutschlandradio durch eine Verwaltungsvereinbarung geregelt werden muss. Mit einer solchen Vereinbarung werden die organisatorische Anbindung des Rundfunkdatenschutzbeauftragten, die finanzielle Ausstattung, die Aufteilung der Kosten sowie die Sicherstellung der erforderlichen Finanzkontrolle geregelt.

An dieser Stelle wird darüber informiert, dass die Verwaltungsvereinbarung nunmehr auch unter Berücksichtigung des rbb zum 23.11.2023 final durch die beteiligten Intendantinnen und Intendanten unterzeichnet werden konnte. Insofern besteht nunmehr Rechtssicherheit. Wichtig ist für mich insbesondere, dass die Federführung dem MDR obliegt. Damit ist auch klar, dass meine Dienststelle bei der Geschäftsstelle von Rundfunk- und Verwaltungsrat des MDR eingerichtet wird, so, wie es § 39 Abs. 2 des MDR-Staatsvertrags vorsieht. Folglich bin ich organisatorisch an den MDR angebunden, dies jedoch unter Berücksichtigung meiner Unabhängigkeit als Aufsichtsbehörde.

Verknüpft mit dieser Anbindung ist die Nutzung der technischen Infrastruktur des Mitteldeutschen Rundfunks. Dies erforderte den Abschluss eines angepassten Auftragsverarbeitungsvertrags, da der Rundfunkdatenschutzbeauftragte als unabhängige Aufsichtsbehörde nicht Teil des MDR ist und insofern in datenschutzrechtlicher Hinsicht verantwortlich ist. Ein solcher Auftragsverarbeitungsvertrag konnte bereits im Frühjahr 2023 vereinbart werden, der die Rechte und Pflichten dahingehend regelt, dass der MDR im Hinblick auf die Datenverarbeitung des Rundfunkdatenschutzbeauftragten weisungsabhängig agiert.

2 Aufgaben und Befugnisse des RDSB

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, Deutschlandradio und ZDF ist geregelt, dass die vom Verwaltungsrat ausgeübte Dienstaufsicht diese Unabhängigkeit keinesfalls beeinträchtigen darf. Nach § 27 Abs. 5 Landesdatenschutzgesetz BW 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 Datenschutzbeauftragte zuständig für die Einhaltung des Datenschutzes bei den Rundfunkanstalten in ihren gesamten Tätigkeiten, aber auch bei deren Beteiligungsunternehmen. 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 seiner 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 er an der Sensibilisierung der Verantwortlichen, der betroffenen Personen und der Öffentlichkeit mitzuwirken hat, und postuliert ebenso die Pflicht, mit anderen Aufsichtsbehörden zusammenzuarbeiten.

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 ist ebenso 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

verhängen (vgl. bspw. § 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.[2]

2.1 Internetauftritt des Rundfunkdatenschutzbeauftragten

Mein Vorgänger im Amt hatte eine sehr ausführliche Internetseite erstellt, die technisch mit den Systemen des rbb verknüpft war. Im Zuge der Übernahme dieser Tätigkeit war es aufgrund der Anbindung meiner Dienststelle an den Mitteldeutschen Rundfunk erforderlich, auch diese Website „umzuziehen“. Hier habe ich gelernt, dass dies nicht „per Knopfdruck“ und mit einer einmaligen Datenübertragung möglich ist, sondern dass nicht unerhebliche technische Hürden zu überwinden und auch viele Entscheidungen zu treffen sind, wie eine solche Website auszusehen hat. Schließlich ist es gelungen, mit tatkräftiger Hilfe der Bereiche des rbb und auch jener des MDR, die inhaltlich, optisch und technisch überarbeitete Website online zu bringen. Damit wird insbesondere auch der Pflicht der Aufsichtsbehörde nachgekommen, die Öffentlichkeit über den Datenschutz zu informieren. Hier ist der Webauftritt zu finden: Website des Rundfunkdatenschutzbeauftragten.

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

2.2 Vorstellung in den Direktorien

Wenngleich ich als Rundfunkdatenschutzbeauftragter des MDR bereits seit 2018 in diese Rolle hineingewachsen bin, so kamen mit Anfang des Jahres 2023 insgesamt sechs Rundfunkanstalten hinzu (der rbb wurde meiner Aufsicht erst Mitte des Jahres 2023 zugeordnet). Daher habe ich es als meine Pflicht erachtet, mich möglichst zeitnah in den Geschäftsleitungen oder Direktorien der von mir beaufsichtigten Rundfunkanstalten vorzustellen.

Unter Berücksichtigung der gesetzlichen und staatsvertraglichen Eigenarten jeder Rundfunkanstalt habe ich die Aufgaben und Befugnisse der Datenschutzaufsicht skizziert und im Rahmen eines Vortrages Schwerpunktsetzungen und wichtige datenschutzrechtliche Themen dargestellt und erläutert. Dies natürlich immer ohne Anspruch auf Vollständigkeit, da - auch dies betone ich stets aufs Neue - das Datenschutzrecht eine teilweise unvorhersehbare Dynamik aufweist.

Ich habe insbesondere die Themen Datenschutzmanagement, Überprüfung von Apps und die Ankündigung des Nutzungsmessungsaudits beleuchtet, aber auch meine Überzeugung bekräftigt, dass Datenschutzaufsicht ebenso auch Unterstützung, Beratung und Hilfestellung bedeutet. Deswegen soll meine Amtszeit auch geprägt sein von der Veröffentlichung von Orientierungshilfen und Positionspapieren möglichst gemeinsam mit der RDSK, aber auch mit dem AK DSB, damit die praktischen Anforderungen stets mit einfließen können. Die Drittplattformen wie Facebook, Tiktok und Instagram müssen auch datenschutzrechtlich immer im Blick gehalten werden, ebenso das Thema Personalisierung und natürlich das das Jahr beherrschende Thema Künstliche Intelligenz. Letzterem hat sich die RDSK bereits relativ früh im Jahr 2023 angenommen und eine erste Orientierungshilfe erstellt, die den Rundfunkanstalten bei der Implikation solcher Tools die Möglichkeit gibt, auch die Sicht des Datenschutzes zu beachten. Hierüber wird unter Kapitel 6.2 und auch 7.2.3 genauer berichtet.

Zentrales Thema ist die Etablierung eines Datenschutzmanagements, das die Funktionsfähigkeit des Datenschutzes in den einzelnen Häusern durch klar geregelte Verantwortlichkeiten, Abläufe und Strukturen sicherstellen soll. Ich habe deutlich darauf hingewiesen, dass es sich um eine Managementaufgabe handelt, was im Ergebnis bedeutet, dass die Geschäftsleitungen unmittelbar für die Umsetzung eines solchen Systems verantwortlich sind. Im laufenden Jahr 2024 werde ich mir die Umsetzung in den Rundfunkanstalten anschauen und hoffe, durch diesen Überblick auch Hinweise geben und zur beschleunigten Umsetzung beitragen zu können. Im Berichtsjahr wurde überdies im Oktober ein Empfehlungspapier zu einem Datenschutzmanagementsystem des AK DSB finalisiert (siehe Kapitel 8.2), an dem auch die Aufsicht mitgewirkt hat. Hier werden die wesentlichen Eckpunkte zur Etablierung dargelegt und die essentiellen Inhalte beschrieben. Ich habe den Eindruck gewinnen können, dass die Geschäftsleitungen der Rundfunkanstalten dem Thema aufgeschlossen

gegenüberstehen, es jedoch fast überall noch Handlungsbedarf gibt. Ich hoffe, dass es mir gelungen ist, den Datenschutz als wichtigen Punkt auf die Agenda der Geschäftsleitungen zu setzen, sodass auch die mit der Umsetzung betrauten Mitarbeitenden mit mehr Verständnis und Unterstützung rechnen können.

3 Entwicklungen im Datenschutzrecht

Gesetzgeberische Entwicklungen fanden im Jahr 2023 hauptsächlich auf europäischer Ebene statt; dort jedoch weniger im originären Regelungsregime des Datenschutzrechts, als vielmehr durch die datenwirtschaftlich geprägte EU-Datenstrategie. Diese beinhaltet mehrere Rechtsakte, die teilweise bereits Geltung entfaltet haben, sich teilweise aber auch noch im Gesetzgebungsprozess befinden. Darüber hinaus wurde mit dem Data Privacy Framework zwischen der EU und den USA ein Nachfolger des „Privacy Shields“ geschaffen, der Datenübertragungen in die USA rechtsicher ermöglichen soll.

3.1 EU-Datenstrategie

Innovationspotentiale im Datenwirtschaftsrecht sollen im Rahmen der europäischen Datenstrategie durch eine Regulierung von Datenzugangsrechten, Datenverträgen und Interoperabilitätsregelungen, neben dem bestehenden datenschutzrechtlichen Rahmen der DSGVO, freigelegt werden. Die damit bezweckte Verstärkung des Datenhandels und die Förderung des Teilens von Daten führen zweifelsohne zu Reibungspunkten mit der Datenschutzgrundverordnung und ihrem persönlichkeitsrechtlichen Schutzgedanken als Ausprägung des Grundrechts auf informationelle Selbstbestimmung. Das sich nun formierende Datenwirtschaftsrecht auf europäischer Ebene soll nach seiner Zielsetzung jedoch keinen ausufernden Datenzugang ermöglichen, sondern entgegenstehende Interessen und damit gerade die Grenzen des Datenzugriffs mitdenken und möglichst effektiv abbilden. (Ob dies tatsächlich gelingt, bleibt nach Erfahrungen in der Anwendung dieser Gesetze abzuwarten.) Deutlich wird die Bedeutung des Datenschutzes auch daran, dass all diese Rechtsakte Unberührtheitsklauseln bezüglich der DSGVO enthalten. Das bedeutet, dass die DSGVO in vollem Umfang gilt und nicht durch diese Gesetze und Verordnungen eingeschränkt wird. Das europäische Datenschutzrecht wurde damit in seinem besonderen Gewicht bekräftigt.

3.1.1 Digital Services Act (DSA)

Ziel des seit 17.02.2024 geltenden Digital Services Act ist die Gewährleistung eines sicheren, vorhersehbaren und vertrauenswürdigen Online-Umfelds und das Funktionieren des Binnenmarktes (Art. 1 Abs. 1 DSA). Damit gemeint ist eine Eindämmung von Hetze, Hass und politischem Extremismus im Internet und in sozialen Netzwerken, erwirkt durch verbindliche Verhaltensvorschriften und Haftungsregeln für Vermittlungsdienste, Hosting-Dienste und Online-Plattformen.

Angebote des öffentlich-rechtlichen Rundfunks können dem Anwendungsbereich des DSA unterfallen. Das betrifft insbesondere interaktive Angebote, wie Kommentar- und Chat-Funktionen oder Hosting-Dienstleistungen, nicht jedoch das Online-Angebot der Mediatheken oder Audiotheken. Denn für die Eröffnung des Anwendungsbereichs kommt es darauf an, ob die Nutzenden auf den eigenen Portalen der Rundfunkanstalten Informationen speichern und verbreiten können – das betrifft interaktive Funktionen beispielsweise innerhalb der eigenen Apps. Darüber hinaus betrifft der DSA die Rundfunkanstalten lediglich als geschäftlicher Nutzer von großen Online-Plattformen. Dabei profitieren auch die Rundfunkanstalten von den Verpflichtungen, die die Online-Plattformen (z. B. Facebook, Instagram, X, TikTok) treffen. Eine mit dem Datenschutzrecht vergleichbare Figur der gemeinsamen Verantwortlichkeit kennt der DSA nicht.

Die als besonders groß eingestuften Plattformen und Suchmaschinen werden direkt von der EU-Kommission beaufsichtigt. Grundsätzlich gilt laut DSA: Je größer die Plattform oder Suchmaschine und damit auch je größer die von diesem Dienst aufgrund dieser Marktmacht ausgehenden Gefahren sind, desto strenger sind die Regulierung und die damit einhergehenden einzuhaltenden Pflichten für diese Diensteanbieter. Für die Durchsetzung des als EU-Verordnung auch in Deutschland direkt anwendbaren DSA wurde ergänzend auf Bundesebene das Digitale-Dienste-Gesetz (DDG) verabschiedet. Auf das Handbuch der Europäischen Rundfunkunion (EBU)[3] mit ausführlichen Erläuterungen zur Anwendbarkeit der für einen Dienst jeweils zutreffenden Pflichten sei an dieser Stelle hingewiesen.

Als zentrale Stelle der Überwachung über die Einhaltung der Regelungen von DSA und DDG soll nach dem Willen des Gesetzgebers die Bundesnetzagentur eingesetzt werden. Eine damit auch den öffentlich-rechtlichen Rundfunk betreffende Aufsicht durch die Bundesnetzagentur sehen die Rundfunkanstalten - aus meiner Sicht zu Recht - kritisch, da, wie auch in der datenschutzrechtlichen Aufsicht durch die Rundfunkdatenschutzbeauftragten, der Grundsatz der Staatsferne im öffentlich-rechtlichen Rundfunk einer staatlichen Aufsicht entgegensteht.

[3] https://www.ebu.ch/guides/open/digital-services-act-handbook-public-version

3.1.2 Digital Markets Act (DMA)

Bereits seit 02.05.2023 gilt der Digital Markets Act. Nach Art. 1 Abs. 1 DMA will diese Verordnung sicherstellen, dass die Märkte des Digitalsektors in der EU trotz der Präsenz von Gatekeepern bestreitbar[4] und fair werden („contestable and fair markets“) und ein reibungsloser Binnenmarkt gewährleistet wird. Der DMA soll damit die Funktionsfähigkeit des Binnenmarkts absichern und der Fragmentierung von Digitalmärkten vorbeugen (Erwgr. 7 S. 2-4 DMA).

Hintergrund ist die Neigung und der Marktmechanismus von Plattformen, wegen der spiralartigen Netzwerkeffekte und rasch eintretenden Größenvorteile, Märkte zum Kippen zu bringen („tipping“). Das bedeutet: Nach dem Winner-takes-all-Prinzip etabliert sich im Markt nur eine Plattform, bei der sich die Nutzer konzentrieren.[5]

Der DMA soll diese Marktmechanismen aufbrechen, auch da sich das Kartellrecht in diesem Bereich als wenig schlagkräftig erwiesen hat. Konkret sollen die Monopole der Big Five (GAMAM = Google, Amazon, Meta, Apple und Microsoft) aufgebrochen werden.

Die Verordnung richtet sich daher gezielt an zentrale Plattformdienste (Gatekeeper/Torwächter – definiert in Art. 2 Nr. 1 DMA), die in den Märkten des digitalen Sektors wichtige Elemente darstellen, aber zugleich auch für den überwiegenden Teil von Beziehungen zwischen Endnutzern und gewerblichen Nutzern zuständig sind. Dazu gehören z. B. Online-Vermittlungsdienste, Online-Suchmaschinen, Online-Dienste sozialer Netzwerke und Video-Sharing-Plattform-Dienste.[6]

Der Begriff Märkte des digitalen Sektors bezieht sich dabei gemäß Art. 2 Nr. 4 DMA auf „alle Produkte und Dienstleistungen, die durch Dienste der Informationsgesellschaft“ bereitgestellt werden. Damit sind wie beim DSA nur kommerzielle Dienste umfasst.

Der DMA regelt, welche Unternehmen als Gatekeeper (Torwächter) in Märkten des digitalen Sektors reguliert werden und sieht für diese eine Reihe von Verboten und Pflichten vor, dabei fordert der DMA die geschäftliche und auch technische Umsetzung dieser Pflichten, ähnlich wie die DSGVO („compliance by design“, Erwgr. 58). Die Sanktionen sind erheblich.[7]

[4] Als „bestreitbar“ wird die Offenhaltung von Märkten und die Eröffnung von Chancen für Wettbewerber verstanden.
[5] Podszun/Bongartz/Kirk, Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie, NJW 2022, 3249
[6] Albrecht, Digital Markets Act kommt – Regulierung von Plattformen und Auswirkungen auf Unternehmen, GWR 2022, 181
[7] Seip/Berberich, Der Entwurf des Digital Markets Act, GRUR-Prax 2021, 44

Als Gatekeeper werden nach Art. 3 Abs. 1 DMA Betreiber zentraler Plattformdienste benannt, die a) erhebliche Auswirkungen auf den Binnenmarkt haben[8], b) einen zentralen Plattformdienst betreiben, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient, und c) hinsichtlich ihrer Tätigkeiten eine gefestigte und dauerhafte Position innehaben oder bei denen absehbar ist, dass sie eine solche Position in naher Zukunft erlangen werden.

Für den öffentlich-rechtlichen Rundfunk ist eine unmittelbare Anwendbarkeit des DMA zu verneinen, da die Eigenschaft als Gatekeeper nicht erfüllt ist und es zudem in den allermeisten Fällen auch an der Kommerzialität fehlt. Die DSGVO bleibt ausdrücklich nach Art. 12 DMA unberührt.

Positive Veränderungen ergeben sich für die Rundfunkanstalten als Nutzer dieser Plattformen. So dürfen Gatekeeper ihre eigenen Angebote nicht mehr bevorzugen (mehr Fairness), Unternehmen erhalten Zugang zu den Daten, die sie über Gatekeeper-Plattformen generieren (mehr Transparenz) und Gatekeeper müssen Unternehmen ermöglichen, Geschäftsbedingungen anzupassen, ihr Angebot zu bewerben und Kundenverträge außerhalb der Plattform abzuschließen (mehr Rechtssicherheit). Das soll für die Konsumenten durch fairen Wettbewerb mittelbar zu mehr Verbraucherschutz, mehr Datenschutz und insgesamt mehr Auswahl führen.

3.1.3 Data Governance Act (DGA)

Der seit 24.09.2023 Geltung entfaltende Data Governance Act (DGA) sieht die Schaffung von Datenräumen innerhalb der EU für die gemeinsame Nutzung und Bündelung von Daten vor. Er zielt damit darauf ab, den grenzüberschreitenden digitalen Binnenmarkt zu fördern, gleiche Wettbewerbsbedingungen in der Datenwirtschaft zu gewährleisten und zu erreichen, dass der Wettbewerb zwischen Unternehmen auf der Qualität der angebotenen Dienstleistungen und nicht auf der Ansammlung von Daten beruht (Erwgr. 2 Abs. 2 S. 4 DGA).[9]

Das heißt, die Regelungen des DGA sollen die bessere Nutzbarmachung existierender Datenbestände durch Weitergabe an und das Teilen mit Dritte(n) fördern und adressieren vordergründig den B2B-Bereich (Datenintermediäre). Durch einheitliche Rahmenbedingungen

[8] digitale Plattformen mit mehr als 6,5 Milliarden Euro Jahresumsatz, beziehungsweise 65 Milliarden Euro Marktwert, mehr als 45 Millionen Endnutzern monatlich in der Europäischen Union und mehr als 10.000 gewerblichen Anbietern auf der Plattform

[9] Kraul, Das neue Recht der digitalen Dienste, § 2, Rn. 52

sollen Innovationsanreize geschaffen werden.[10] Zudem soll das Vertrauen in den freiwilligen Datenaustausch zum Nutzen von Unternehmen und Bürgern gestärkt werden.[11]

Vom sachlichen Anwendungsbereich erfasst sind sowohl personenbezogene als auch nicht-personenbezogene Daten. Der persönliche Anwendungsbereich erstreckt sich auf die in Art. 1 Abs. 2 S. 2 DGA genannten Bereiche: öffentliche Stellen (Art. 2 Nr. 17 DGA)[12] , Anbieter von Datenvermittlungsdiensten (Art. 2 Abs. 1 Nr. 11 DGA) und anerkannte Einrichtungen, die Datenaltruismus-Dienste (Art. 2 Nr. 16 DGA)[13] erbringen. Dem liegt u.a. die Vorstellung zugrunde, dass auch geschützte Daten, die mithilfe öffentlicher Gelder generiert oder gesammelt wurden, der Gesellschaft zugutekommen sollen, was bisher vor allem mangels einheitlicher Rahmenbedingungen nicht möglich war (Erwgr. 6 DGA).

Für die Rundfunkanstalten kommt eine Anwendbarkeit als „öffentliche Stelle“ bzw. konkreter als „Einrichtung des öffentlichen Rechts“ (Art. 2 Nr. 18 DGA) in Betracht. Voraussetzungen sind eine Aufgabenerfüllung im allgemeinen Interesse, das Vorliegen von Rechtspersönlichkeit und einer überwiegenden Finanzierung durch die öffentliche Hand bzw. einer staatlich geprägten Aufsicht (Staatsnähe).

Die öffentlich-rechtlichen Rundfunkanstalten erfüllen mit ihrem auf Art. 5 Abs. 1 S. 2 GG gestützten Funktionsauftrag einen nicht gewerblichen und im allgemeinen Interesse liegenden Zweck und besitzen als juristische Personen des öffentlichen Rechts Rechtspersönlichkeit.

Fraglich ist die Erfüllung des Kriteriums der Staatsnähe, denn der öffentlich-rechtliche Rundfunk in Deutschland unterliegt gerade dem Gebot der Staatsferne. Voraussetzung für die Erfüllung dieses in Art. 2 Nr. 17 lit c) DGA beschriebenen Kriteriums der Staatsnähe ist jedoch das Vorliegen einer lediglich potenziellen Einflussnahme durch staatliche Stellen; einer tatsächlichen Einflussnahme bedarf es nicht.[14] Nach dem EuGH Urteil vom 13.12.2007 (C-337/06) sind die öffentlich-rechtlichen Rundfunkanstalten nach weitgehend überschneidender Definition wie im DGA als öffentliche Auftraggeber im Sinne des § 99 Nr. 2 Gesetz gegen Wettbewerbsbeschränkungen (GWB) anzusehen. Die notwendige Staatsverbundenheit der Rundfunkanstalten ergibt sich aus ihrer überwiegenden

[10] Specht-Riemenschneider, in: Specht/Hennemann, Data Governance Act, 1. Aufl. 2023, DGA Art. 1, Rn. 9
[11] https://digital-strategy.ec.europa.eu/de/policies/data-governance-act-explained
[12] Staat, Gebietskörperschaften, Einrichtungen des öffentlichen Rechts oder Verbände, die aus einer oder mehreren dieser Körperschaften oder einer oder mehreren dieser Einrichtungen des öffentlichen Rechts bestehen
[13] In Art. 2 Nr. 16 DGA definiert und meint die freiwillige und entgeltfreie Datenbereitstellung durch Einzelpersonen oder Unternehmen zum Wohl der Allgemeinheit (z.B. die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die bessere Erbringung öffentlicher Dienstleistungen oder bessere staatliche Entscheidungsfindung, siehe Erwgr. 45). Beispiele aus der Praxis sind die Projekte „OpenSCHUFA“ von Algorithmwatch oder die Corona-Datenspende-App des Robert-Koch-Institus.
[14] Specht-Riemenschneider, in: Specht/Hennemann, Data Governance Act, 1. Aufl. 2023, DGA Art. 2, Rn. 138

Finanzierung durch hoheitlich auferlegte Zwangsbeiträge (Rundfunkbeitrag), der keine spezifische Gegenleistung gegenüber steht.[15] Die verfassungsrechtliche Verankerung der Staatsferne bestimmter Einrichtungen bzw. ihrer Freiheit von politischem Einfluss schließt laut EuGH ihre Auftraggebereigenschaft nicht aus.[16]

Damit fallen auch die Rundfunkanstalten (Funktionsauftrag des öffentlich rechtlichen Rundfunks) **unter die Definition der im DGA bezeichneten Einrichtungen des öffentlichen Rechts.[17] Der Anwendungsbereich des DGA ist somit grundsätzlich eröffnet**.

Aber: Der **Anwendungsbereich** wird gemäß Art. 3 Abs. 2 lit. b) DGA **eingeschränkt**. Danach gelten die Art. 3 - 9 DGA (Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen) **nicht hinsichtlich der Daten, die im Besitz öffentlich-rechtlicher Rundfunkanstalten** und ihrer Zweigstellen oder anderer Stellen und deren Zweigstellen sind und **der Wahrnehmung eines öffentlichen Sendeauftrags dienen.**

„Sendeauftrag“ wird von der EU jedoch nicht eindeutig definiert, entspricht aber ungefähr dem deutschen Verständnis des Auftrags des öffentlich-rechtlichen Rundfunks nach §§ 2 Abs. 1 S. 1, 26 MStV.[18]

„[…] im Besitz […]“ meint die technisch-faktische Herrschaft über die Daten, die der Wahrnehmung des Sendeauftrags dienen.[19] Umfasst sind damit alle Daten, die zur Durchführung des Rundfunkauftrags verwendet werden. Ein rechtssicherer Umgang kann hier nur durch eine weite Auslegung dieser Voraussetzung verwirklicht werden.

Der DGA ist demnach nur für die Rundfunkanstalten und deren Gemeinschaftseinrichtungen anwendbar, wenn die jeweiligen Daten nicht zur Wahrnehmung des Sendeauftrags dienen. Welche Daten darunter im Einzelnen zu verstehen sind, ist zu prüfen.

Eine Anwendbarkeit für Beteiligungsunternehmen kommt bei weiter Auslegung als öffentliche Einrichtung im Sinne der Definition in Art. 2 Nr. 18 DGA ggf. in Betracht, jedoch nur, wenn das

[15] Siehe auch: Dörr, in: Beck'scher Vergaberechtskommentar, 4. Aufl. 2022, GWB § 99, Rn. 94
[16] EuGH 13.12.2007 – C-337/06, Slg. 2007, I-11173, Rn. 31
[17] „Einrichtungen des öffentlichen Rechts umfassen (öffentlich-rechtliche) Kultur- und Bildungseinrichtungen wie Bibliotheken, Archive, Museen, Orchester, Opern, Ballette und Theater sowie öffentlich-rechtliche Rundfunkanstalten und ihre Tochtergesellschaften“ (Specht-Riemenschneider, in: Specht/Hennemann, Data Governance Act, 1. Aufl. 2023, DGA Art. 2, Rn. 147)
[18] Specht-Riemenschneider, in: Specht/Hennemann, Data Governance Act, 1. Aufl. 2023, DGA Art. 3, Rn. 49
[19] Specht-Riemenschneider, in: Specht/Hennemann, Data Governance Act, 1. Aufl. 2023, DGA Art. 3, Rn. 53

Unternehmen nicht gewerblich oder kommerziell geprägt ist. Damit ist der Raum für eine Anwendbarkeit in diesem Bereich sehr klein.

Darüber hinaus kommt eine Anwendbarkeit für Beteiligungsunternehmen nur potentiell in Betracht, wenn ein angemeldeter Datenvermittlungsdienst nach Art. 10 ff. DGA erbracht wird.

Im Ergebnis ergeben sich für die Rundfunkanstalten begrenzte Pflichten zur Datenweiterverwendung bzw. zum Datenzugang gemäß Art. 4, 5 DGA für Daten, die nicht dem Sendeauftrag unterfallen. Eine DSGVO-Unberührtheitsklausel ist in Art. 1 Abs. 3 DGA enthalten.

3.1.4 Data Act (DA)

Der ab 11.01.2024 in Kraft getretene Data Act (DA) regelt den Zugang und die Nutzung von Daten, die beim Einsatz von Produkten und Diensten generiert werden. Die meisten Regelungen des DA gelten jedoch erst ab September 2025.

Neben dem besseren Datenzugang soll die Datenproduktion insgesamt gefördert werden, um die Datenverfügbarkeit im Markt zu erhöhen und Datensilos aufzubrechen. Der branchenübergreifende Datenaustausch zwischen Unternehmen sowie zwischen Unternehmen und staatlichen Institutionen soll verbessert werden.

Als Querschnittsmaterie zwischen Datenschutzrecht und Datenhandel soll der Data Act Rücksicht sowohl auf die Grundsätze der Datenminimierung und des Datenschutzes (Erwgr. 8 S. 1 DA) als auch auf die Vorteile der Zuweisung von Zugangs- und Nutzungsrechten (Erwgr. 6 S. 3 DA) nehmen.[20]

Der Data Act findet auf Daten Anwendung, die bei der Nutzung eines Produkts oder verbundenen Dienstes (Internet of Things) erzeugt werden.

Adressaten des Data Act sind gemäß Art. 1 Abs. 3 DA Hersteller und Nutzer von Produkten (etwa mit dem Internet verbundene Haushaltsgeräte, Fahrzeuge oder Industriemaschinen) und Diensten (Software, ohne die ein Produkt seine Funktionen nicht ausführen könnte) sowie Dateninhaber, die Daten bereitstellen, Datenempfänger, öffentliche Stellen und Einrichtungen der EU, die Daten erhalten, und Anbieter von Datenverarbeitungsdiensten.

[20] Kraul, Das neue Recht der digitalen Dienste, § 2 Ziele, Anwendungsbereich und Verhältnis zu anderen Rechtsakten, Rn. 57; siehe auch zum Überblick : https://www.zeit.de/digital/2023-06/data-act-eu-parlament-datengesetz-big-tech-unternehmen-faq?utm_referrer=https%3A%2F%2Fwww.google.com%2F

Für Dateninhaber, also juristische oder natürliche Personen, die je nach Datenart berechtigt, verpflichtet oder dazu fähig sind, Daten bereitzustellen (vgl. Art. 2 Nr. 13 DA), sieht der DA in Art. 3-5 Pflichten zur Zugänglichmachung von nutzergenerierten Daten vor.[21] Träger von personenbezogenen sowie nicht-personenbezogenen Informationen sind gleichermaßen erfasst.

Die Rundfunkanstalten und ebenso die Gemeinschaftseinrichtungen und Tochterunternehmen sind als potentielle Nutzer, Dateninhaber, Datenempfänger bzw. als öffentliche Stelle (Auslegung vergleichbar zu DGA, insofern sind Tochterunternehmen keine öffentliche Stelle) **vom Anwendungsbereich betroffen. In der Regel wird eine Betroffenheit aber nur als Nutzer relevant.** Als Hersteller von Produkten und Diensten bzw. Dateninhaber und Datenempfänger käme eine Anwendung nur in Betracht, wenn vernetzte Produkte und dazugehörige digitale Dienste entwickelt oder vertrieben werden.

Der DA setzt auf wettbewerbliche Instrumente, insbesondere Zugangsrechte sowie Leitplanken für Datenverträge, statt auf absolute Rechte an Daten (wie das lange diskutierte Dateneigentum, etc.).

Allein die Nutzer vernetzter Geräte sollen darüber entscheiden können, wie mit Daten umgegangen werden soll, an deren Entstehung sie mitgewirkt haben. Nutzer können dabei Unternehmen wie auch Verbraucher sein. Der Data Act soll es den Nutzern ermöglichen, diese Daten auszuwerten und unter bestimmten Bedingungen an Dritte (Art. 5 DA) weiterzugeben.[22]

Hauptziel des DA ist ein fairer Datenzugang sowie eine faire Datennutzung, damit steht der DA automatisch im Spannungsverhältnis mit dem möglichst umfassenden Schutz personenbezogener Daten aus der DSGVO. Um diese Widersprüche in Einklang zu bringen, schränkt der DA den Anwendungsbereich für personenbezogene Daten ein. Personenbezogene Daten dürfen nur den betroffenen Personen oder bei Vorliegen einer datenschutzrechtlichen Rechtsgrundlage (Art. 6 DSGVO) auch an Dritte zur Verfügung gestellt werden. Auch der Data Act enthält eine DSGVO-Unberührtheitsklausel in Art. 1 Abs. 5 DA.

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

Neben den beschriebenen Rechtsakten unter der Überschrift der europäischen Datenstrategie gehörte im Jahr 2023 die angestrebte Regulierung von „Künstlicher Intelligenz“ zu den herausgehobenen Themen der EU-Gesetzgebung. Die KI-Verordnung wurde nun am 13.03.2024 durch das Europäische Parlament verabschiedet und hat sich zum Ziel gesetzt, insbesondere eine

[21] Kraul, Das neue Recht der digitalen Dienste, § 2 Ziele, Anwendungsbereich und Verhältnis zu anderen Rechtsakten, Rn. 58

[22] https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/dihk-durchblick-digital/data-act-63748

rechtssichere, innovationsermöglichende und vertrauenswürdige Nutzung (sicher, transparent, ethisch, unparteiisch und unter menschlicher Kontrolle) generativer Künstlicher Intelligenz zu ermöglichen.[23]

Die KI-Verordnung verfolgt einen risikobasierten Ansatz zur Differenzierung der Anforderungen an KI-Anbieter und KI-Nutzer. Die in der Regulierung abgestuften Risikogruppen werden bezeichnet als: 1. Verbotene Praktiken (Art. 5 KI-VO), 2. Hochrisiko-KI-Systeme (Art. 6 ff. KI-VO), 3. bestimmte KI-Systeme, die mit natürlichen Personen interagieren (Art. 52 KI-VO), 4. minimales Risiko oder kein Risiko (keine speziellen Regelungen).

Bei Nichtbeachtung der Anforderungen können Sanktionen, wie z.B. Bußgelder erhoben werden (Art. 71 f. KI-VO). Zudem wird an einer KI-Haftungs-Richtlinie (AI Liability Directive – Entwurf vom 28.09.2022[24]) gearbeitet, um darüberhinausgehenden Haftungsfragen zu klären und um durch künstliche Intelligenz geschädigte Personen beim gerichtlichen Nachweis zu entlasten.

Durch die datengetriebene Funktionsweise von KI muss bei jeglichen Regulierungsansätzen auch das Datenschutzrecht entsprechend und mit hoher Priorität mitgedacht werden. Auch wenn die DSGVO von der KI-Verordnung nach der Gesetzesbegründung unberührt bleibt, könnte die KI-VO Auswirkungen auf die Anwendung der DSGVO haben. Hier wird die Praxis zeigen, wie die beiden Regelungssysteme nebeneinander angewendet werden.

3.2 Data Privacy Framework

Auf den Angemessenheitsbeschluss der EU für den Datenschutzrahmen zwischen der Europäischen Union und den USA vom 10. Juli 2023 und die Befassung der RDSK mit diesem Thema wird unter Kapitel 7.2.2 dieses Berichtes ausführlich eingegangen. Daher wird zur Vermeidung von Wiederholungen auf dieses Kapitel verwiesen.

3.3 Entwurf TTDSG-VO

Das Bundesministerium für Digitales und Verkehr (BMDV) hat zum Referentenentwurf der „Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Telemedien-

[23] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de
[24] https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

Datenschutz-Gesetz (Einwilligungsverwaltungsverordnung – EinwV)“ ein Anhörungsverfahren eingeleitet. Mit einer so bezeichneten „Cookie-Reform“ möchte das BMDV ein nutzerfreundliches und wettbewerbskonformes Einwilligungsmanagement etablieren.[25]

Mit Blick auf die Betroffenheit des öffentlich-rechtlichen Rundfunks wurde mir Gelegenheit zur Stellungnahme zum Referentenentwurf der TTDSG-VO gegeben.

Der Verordnungsentwurf betrifft die Einwilligungsverwaltung und damit die Ausgestaltung der §§ 25 Abs. 1 und 26 Abs. 1 TTDSG. Eine besondere Betroffenheit bezüglich des Datenschutzes in den Rundfunkanstalten habe ich insofern zu großen Teilen nicht ausgemacht.

Stellung genommen habe ich allerdings zu § 4 Abs. 4 Nr. 1 TTDSG-VO (Entwurf). Dieser eröffnet die Möglichkeit, dass der anerkannte Dienst zur Einwilligungsverwaltung den Endnutzer auf eine Speicherung von Informationen in der Endeinrichtung des Endnutzers hinweisen kann, wenn dies ohne Einwilligung nach § 25 Abs. 1 TTDSG erfolgt. Vor dem Hintergrund des verfassungsrechtlich zugeschriebenen Auftrags des öffentlich-rechtlichen Rundfunks, sind Einwilligungen zur Speicherung von bestimmten Informationen - zum Beispiel zum Zweck der anonymisierten Nutzungsmessung - gemäß § 25 Abs. 2 Nr. 2 TTDSG nach hiesiger Rechtsauffassung nicht erforderlich. Dies führt aktuell dazu, dass in diesen Konstellationen für die Nutzung von Apps und Websites der öffentlich-rechtlichen Rundfunkanstalten auf Cookie/Consent-Banner verzichtet werden kann. Ich verweise an dieser Stelle auf die Empfehlungen zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten der RDSK vom Juli 2022.

Durch den angesprochenen § 4 Abs. 4 Nr. 1 TTDSG-VO sehe ich das Risiko einer Verunsicherung der Nutzenden von Telemedien des öffentlich-rechtlichen Rundfunks, wenn die Endnutzer durch einen anerkannten Dienst zur Einwilligungsverwaltung auf eine vermeintlich fehlende Einwilligung hingewiesen werden und der falsche Eindruck eines nicht rechtskonformen Angebots entstehen könnte. Für das sensible Vertrauen der Nutzerinnen und Nutzer in den öffentlich-rechtlichen Rundfunk wäre das wenig zuträglich und sollte nach meiner Auffassung vermieden werden.

Ich habe daher in meiner Stellungnahme empfohlen, in § 4 Abs. 4 Nr. 1 TTDSG-VO eine Ausnahme einzufügen, dass kein entsprechender Hinweis erfolgt, wenn die Rechtmäßigkeit der Speicherung von Informationen durch § 25 Abs. 2 TTDSG gewährleistet wird.

Nun bleibt der weitere Verordnungsgebungsprozess zu verfolgen. Bis Ende des Jahres 2023 gab es keine weiteren Informationen vom BMDV.

[25] https://bmdv.bund.de/SharedDocs/DE/Artikel/DP/cookie-reform-ttdsg.html

3.4 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.

Das Jahr 2023 war dabei reich an beachtlicher - auch höchstrichterlicher - Rechtsprechung. Aus der Perspektive meiner Behörde waren insbesondere Entscheidungen im Themenkreis Anonymisierung/Pseudonymisierung (EuG), die weiterhin bestehende Diskussion von IP-Adressen als personenbezogene Daten (EuG, OLG Köln), die Auslegung des Rechts auf Auskunft bzw. Datenkopie gemäß Art. 15 Abs. 1 und 3 DSGVO (EuGH) sowie die Anforderungen an Cookie-Banner (LG München, OLG Köln) relevant und berichtenswert.

3.4.1 Anonymisierung

Die Anonymisierung personenbezogener Daten gilt als eine der effektivsten Maßnahmen des operativen Datenschutzes. Besonders im Rahmen der von meiner Behörde durchgeführten Befragung der verwendeten Nutzungsmessungs-Tools durch die Rundfunkanstalten (siehe Kapitel 6.1.2) war das Thema der Anonymisierung der erhobenen Daten von zentraler Bedeutung, um einen datenschutzgemäßen Einsatz dieser Tools zu prüfen und letztlich sicherzustellen. Es stellt sich dabei konkret die nicht immer leicht zu beantwortende Frage, wann eine Anonymisierungsmethode tatsächlich zu einer faktischen Anonymisierung der Daten führt. Das muss im Einzelfall geprüft werden.

Dazu ist es jedoch zunächst erforderlich, den Begriff der Anonymisierung zu definieren. Im Gesetzestext der DSGVO findet sich im Gegensatz zur Pseudonymisierung keine Begriffsdefinition der Anonymisierung. Allerdings stellt der Erwägungsgrund 26 S. 5 zur DSGVO klar, dass die Grundsätze der DSGVO nicht auf anonyme Informationen Anwendung finden, worunter Informationen zu verstehen sind, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Unterschieden wird also zwischen anonymen Daten, die keinen Personenbezug aufweisen und anonymisierten Daten, die zwar einst personenbezogene Daten waren, aber eine Identifizierung der betroffenen Person durch eine wirksame Anonymisierungsmethode ausschließen.

Die kurze Erläuterung zum Begriffshintergrund ist deshalb wichtig, da die aktuelle europäische Rechtsprechung für die ohnehin umstrittene juristische Auslegung, wann bzw. durch welche technische Maßnahme eine Anonymisierung angenommen werden kann, eine neue Richtung

vorgibt. Denn offen lässt der genannte Erwägungsgrund und auch die DSGVO selbst, ob eine Identifizierbarkeit für jeden objektiv ausgeschlossen sein muss (absolute Anonymisierung) oder ob das Kriterium subjektiv zu betrachten ist und es nur darauf ankommt, ob die Identifizierbarkeit lediglich für den für die Datenverarbeitung Verantwortlichen ausgeschlossen sein muss (faktische oder relative Anonymisierung).

Die Frage der wirksamen Anonymisierung muss also vor allem aus dem umgekehrten Blickwinkel betrachtet werden: Lässt sich die betroffene Person re-identifizieren? Genau diese Frage haben wir im Übrigen auch den Verantwortlichen im Fragebogen zur Nutzungsmessung gestellt.

Wie angesprochen, gab es zum juristischen Verständnis dieser Frage und damit auch zur Definition, wann eine wirksame Anonymisierungsmethode vorliegt, eine richtungsweisende Entscheidung durch das Gericht der Europäischen Union - EuG (Urteil vom 26.04.2023, SRB gegen EDSB, T-557/20). Das EuG bejahte in diesem Urteil die Möglichkeit, dass eine Pseudonymisierung durch einen Verarbeiter für einen Dritten eine anonymisierende Wirkung entfalten kann. Es verwies in der Begründung auch auf die Rechtsprechung des EuGH (Urteil vom 19.10.2016, Breyer, C-582/14), wonach IP-Adressen, die von einem Verarbeiter gespeichert werden, als personenbezogene Daten anzusehen sind, wenn dieser Verarbeiter unter Hinzunahme weiterer Informationen seitens des Internetzugangsanbieters die betroffene Person identifizieren kann. Abgestellt hat der EuGH darauf, dass das Wissen anderer Personen oder Stellen für den Verantwortlichen ein Mittel darstellt, das dieser vernünftigerweise zur Identifizierung der betreffenden Personen nutzen kann. Das EuG sieht im Umkehrschluss zur Aussage des EuGH die Identifizierbarkeit als nicht gegeben an, wenn ein Datenempfänger über kein solches Wissen und ebenso keine Möglichkeit verfügt, die zur Re-Identifikation erforderlichen weiteren Informationen zu erhalten. Das EuG hält damit auch eine relative Anonymisierung für ausreichend, um das Vorliegen personenbezogener Daten im Sinne des Art. 4 Nr. 1 DSGVO und damit die Anwendbarkeit der DSGVO zu verneinen.

Das heißt, dass es bei Übermittlung pseudonymisierter Daten zunächst auf den Einzelfall ankommt und zur Feststellung einer wirksamen Anonymisierung zu untersuchen ist, ob der Empfänger der Daten eine Re-Identifizierung vornehmen kann. Besteht für den Empfänger keine Möglichkeit rechtmäßig an die erforderlichen weiteren Informationen zu gelangen, um die pseudonymisierten Daten zu re-identifizieren, ist nach Auslegung des EuG von anonymisierten Daten auszugehen. Neben der Rechtmäßigkeit der Informationsbeschaffung soll es auch auf den damit verbundenen Aufwand ankommen. Eine Unmöglichkeit der Informationsbeschaffung soll in dieser Hinsicht nicht erforderlich sein, vielmehr soll es nach einer Risikoprognose darauf ankommen, ob es nach Würdigung der Gesamtumstände für den Empfänger mit dem ihm zur Verfügung stehenden Mitteln zu erwarten ist, dass dieser an die Informationen gelangt, die eine Re-Identifizierung ermöglichen.

Zur Sicherstellung einer möglichst unwahrscheinlichen De-Anonymisierung sind insbesondere wirksame technische und organisatorische Maßnahmen von Bedeutung.

Festzuhalten ist, dass die Bewertung der Anonymität bestimmter Daten nach Auffassung des EuG also vom konkreten Verarbeitungskontext abhängig sein soll. Wenn der Dritte die Zuordnungsregel nicht kennt und auch nicht über Zusatzwissen verfügt, das eine Re-Identifizierung zuließe bzw. nicht unter Einsatz eines zu erwartenden verhältnismäßigen Aufwands nach aller Wahrscheinlichkeit an ein erforderliches Zusatzwissen gelangen könnte, wird die Anonymisierungsmethode als wirksam angesehen. Gänzlich neu ist diese Auslegung nicht, liegt sie wie skizziert auf einer Linie mit der angesprochenen EuGH Rechtsprechung (Breyer-Entscheidung 2016, siehe oben). Dennoch bekräftigt und verdeutlicht das Urteil diese Auslegung nochmal in beachtlicher Weise.

Fazit: Es ist zu vermuten, dass sich diese Auffassung des EuG zur anonymisierenden Wirkung der Pseudonymisierung durchsetzt und damit die relative Anonymisierung an Bedeutung gewinnt bzw. die absolute Anonymisierung nicht länger erforderlich ist, um das von der DSGVO geforderte Schutzniveau personenbezogener Daten zu erreichen. Dennoch bleibt eine absolute Anonymisierung die sicherste Variante, um eine Re-Identifizierung auszuschießen und wird von mir ausdrücklich begrüßt, auch da relative Anonymisierungsmethoden bereits seitens der Verantwortlichen mit einem individuellen und damit größeren Prüfungsaufwand (Risikoprognose) je Datenverarbeitungsvorgang verbunden sind. Außerdem besteht bei einer längerfristigen Aufbewahrung der Daten das Risiko, dass sich zum Beispiel durch technischen Fortschritt (Stichwort KI) das Risiko einer Re-Identifizierung mit der Zeit erhöht.

3.4.2 IP-Adresse als personenbezogenes Datum weiter in der Diskussion

Die Diskussion zur IP-Adresse als personenbezogenes Datum bleibt aktuell und wird von der aktuellen Rechtsprechung immer wieder aufgegriffen. Da die IP-Adresse als Gerätekennung die Kommunikation zwischen Geräten über das Internet erst ermöglicht, lässt sich ihre Übertragung technisch nicht vermeiden. Die Einschätzung, ob mit der Übertragung einer IP-Adresse bereits ein personenbezogenes Datum übertragen wird, hat damit erhebliche Relevanz.

In der DSGVO werden IP-Adressen nicht ausdrücklich erwähnt und kommen lediglich in Erwägungsgrund 30 zur DSGVO vor[26]. Dort wird ersichtlich, dass IP-Adressen „insbesondere“ in

[26] „Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.“

Kombination mit weiteren Informationen einen Personenbezug ermöglichen können. Eine Kombination mit weiteren Informationen wird damit vom EU-Gesetzgeber für erforderlich gehalten, um einen Personenbezug herzustellen, ist aber auch nicht zwingend, wie die Formulierung „insbesondere“ erkennen lässt. Ausgeschlossen wird damit jedenfalls nicht a priori, dass eine IP-Adresse für sich genommen bereits ein personenbezogenes Datum sein könnte.

Ausgangspunkt und Status quo in der Rechtsprechung bildet die sogenannte Breyer-Entscheidung des EuGH aus dem Jahr 2016 (Urteil vom 19.10.16, Breyer, C-582/14), auf die sich auch der BGH im Urteil aus dem Jahr 2017 stützt (Urteil vom 16.05.2017 - VI ZR 135/13). Auch das zur Frage der Anonymisierung unter Kapitel 3.1.4 erläuterte Urteil des Gerichts der Europäischen Union (EuG) zur Pseudonymisierung (Urteil vom 26.04.2023, SRB gegen EDSB, T-557/20) wird von dieser Thematik tangiert.

Schnittmenge der grundsätzlichen Entscheidung von EuGH, BGH und EuG ist das relative Verständnis des Personenbezugs. Eine Identifizierung bzw. eine Identifizierbarkeit - und damit die Voraussetzung für ein personenbezogenes Datum gemäß Art. 4 Nr. 1 DSGVO - muss „praktisch durchführbar“, also nicht mit unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft verbunden sein. Ist dies der Fall, wird das verbleibende Risiko einer (Re-)Identifizierung als vernachlässigbar angesehen und ein anonymes bzw. anonymisiertes Datum angenommen, mit der Folge der Nichtanwendbarkeit der DSGVO. Auf eine absolute Nicht-Identifizierbarkeit soll es nicht ankommen.

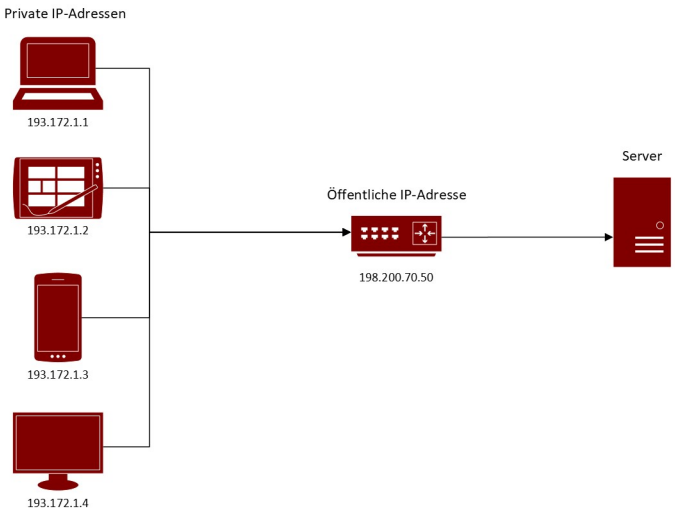
Auf dieser Linie bleibt auch ein aktuelles Urteil des OLG Köln (Urteil vom 03.11.2023 - 6 U 58/23), das dieses relative Verständnis der Anonymisierung heranzieht, um die Frage der IP-Adresse als personenbezogenes Datum ein weiteres Mal zu betrachten und im Ergebnis zu bejahen. Danach stellen nach dem OLG Köln dynamische IP-Adressen, „die ein Anbieter von Online-Diensten speichert, Einzelangaben über sachliche Verhältnisse dar, da die Daten Aufschluss darüber geben, dass zu bestimmten Zeitpunkten bestimmte Seiten bzw. Dateien über das Internet abgerufen wurden. Sie können daher personenbezogene Daten sein (BGH NJW 2017, 2416, 2417, Rn. 18).“

In der zitierten Entscheidung hat der BGH ausgeführt, dass eine dynamische IP-Adresse, die beim Zugriff einer Person auf eine Internetseite gespeichert wird, auch für einen "reinen" Webseitenbetreiber bzw. Anbieter von Online-Mediendiensten ein personenbezogenes Datum darstellt. Begründet wurde das damit, dass der Betreiber der Webseite über rechtliche Mittel verfüge, die vernünftigerweise eingesetzt werden können, um mithilfe Dritter, und zwar der zuständigen Behörde und des Internetzugangsanbieters, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen. Dies ergebe sich daraus, dass diese Betreiber sich insbesondere im Fall von Cyberattacken an die zuständige Behörde wenden könnten, damit diese

die nötigen Schritte unternehme, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten (BGH NJW 2017, 2416, 2417 Rn. 25). Das OLG Köln schließt sich dieser Entscheidung des BGH und damit der EuGH-Rechtsprechung an und erkennt einen Personenbezug an, da das erforderliche Zusatzwissen zur Identifizierung vorhanden ist oder erlangt werden könne.

Die staatlichen Aufsichtsbehörden folgen bisher der Rechtsprechung und nehmen bei IP-Adressen immer einen Personenbezug an[27], ohne dies tiefer zu begründen. In der Literatur finden sich nun jedoch zunehmend Stimmen, die die skizzierten Maßstäbe der Rechtsprechung für eine gegenteilige Auffassung einer Verneinung der IP-Adresse als personenbezogenes Datum heranziehen, zumindest aber einer pauschalen Annahme als personenbezogenes Datum widersprechen.[28]

Technischer Anknüpfungspunkt des Urteils des OLG Köln war eine öffentliche IP-Adresse. Durch eine öffentliche IP-Adresse kann im Grunde nur der Anschlussinhaber identifiziert werden, nicht das konkrete Gerät, das über eine private IP-Adresse untergeordnet wird, die am ehesten noch (aber kaum zweifelsfrei) einen konkreten Nutzer vermuten ließe.



Ein Rückschluss auf eine private IP-Adresse eines Geräts wäre nur denkbar, wenn dem Website-Betreiber auch die Protokolldaten des WLAN-Routers zur Verfügung stünden. Aber selbst dann könnte ein Gerät von mehreren Nutzern eines Haushalts genutzt werden, oder die private IP-

[27] DSK OH Telemedien 2021, Stand 2022, z.B. Rn. 109, 136

[28] Baumgartner, Sind IP-Adressen wirklich immer personenbezogene Daten? Ein Zwischenruf, ZD 2023, 125; sowie Baumgartner, EuG: Bestimmung des Personenbezugs von Daten, ZD 2023, 399; Wildberg/Lee-Wunderlich, It's not personal – Warum IP-Adressen nicht immer personenbezogene Daten sind, CCZ 2023, 281; Schwartmann/Benedikt, OLG Köln: Rechtswidrige Übermittlung der IP-Adresse in die USA, RDV 2024, 29 (30 f.)

Adresse könnte durch den Nutzer zwischenzeitlich geändert worden sein, jedenfalls wird durch die IP-Adresse immer nur der Anschlussinhaber erkennbar, nicht der konkrete Gerätnutzer.[29] Praktisch ist es damit nur in den wenigsten Fällen denkbar, ausschließlich anhand der IP-Adresse eine natürliche Person als im konkreten Fall handelnde Person eindeutig zu identifizieren, sieht man vom eindeutig identifizierbaren aber möglicherweise unbeteiligten Anschlussinhaber ab. Eine negative Auslegung zur Frage der IP-Adresse als personenbezogenes Datum lässt sich damit durchaus gut begründen, führt aber dazu, dass der Anwendungsbereich der DSGVO damit zumindest für öffentliche IP-Adressen ausgeschlossen wäre.

Diese Lesart entspricht zumindest in der Konsequenz bisher nicht der vordergründig zu berücksichtigenden höchstrichterlichen Rechtsprechung durch EuGH und BGH, könnte sich jedoch zukünftig ändern, sollten die mittlerweile anerkannten relativen Anonymisierungsmethoden (siehe das oben genannte Urteil des EuG 2023) auch zu einer relativen Betrachtungsweise des Personenbezugs von Daten, insbesondere bei IP-Adressen führen, was durchaus stringent wäre.

Für die Rundfunkanstalten wäre die Auffassung, IP-Adressen, die losgelöst von weiteren Informationen von Nutzern erhoben werden, nicht mehr als personenbezogenes Datum anzusehen, von großer Bedeutung, insbesondere für die Nutzungsmessung. Für Tools, die lediglich IP-Adressen verarbeiten, käme es dann nicht mehr auf die Anonymisierung dieser IP-Adressen an, um unter die Rechtsgrundlage des Art. 6 Abs. 1 lit. e) DSGVO zu fallen und damit vom Auftrag des öffentlich-rechtlichen Rundfunks gedeckt zu sein. Auch nicht-anonymisierte IP-Adressen könnten dann vorbehaltlich von § 25 Abs. 2 TTDSG ohne Einwilligung erfasst und verarbeitet werden. Insofern empfiehlt es sich, die weitere Entwicklung in der Rechtsprechung und Gesetzgebung genau zu beobachten. Um es aber zu bekräftigen: **Aktuell empfehle ich, IP-Adressen weiterhin als personenbezogene Daten anzusehen, um eine in jedem Fall datenschutzkonforme und rechtssprechungssichere Verarbeitung zu gewährleisten.**

3.4.3 Ausgestaltung von Cookie-Bannern

Das Landgericht München I beschäftigte sich Ende des Jahres 2022 mit der rechtmäßigen Gestaltung von Cookie-Bannern (Urteil vom 29.11.2022, Az.: 33 O 14776/19). Dabei ging es insbesondere darauf ein, wie ein Zwei-Ebenen-Banner ausgestaltet sein sollte, um die gesetzliche Anforderung der Freiwilligkeit der Einwilligung (vgl. Art. 4 Nr. 11 DSGVO) zu erfüllen.

[29] So auch: Baumgartner, ZD 2023, 125 (126) (der sogar von Missverständnis zwischen EuGH und BGH spricht); Schwartmann/Benedikt, RDV 2024, S. 29 (31).

Nach der Urteilsbegründung ist eine Einwilligung dann nicht freiwillig, wenn der Nutzer diese lediglich im vollem Umfang erteilen und durch Betätigung der Schaltfläche „Einstellungen“ eine gesonderte Auswahl treffen, die Website ansonsten aber nicht nutzen kann (vgl. Rn. 112).

Es wird im Urteil als erheblich erachtet, ob zumindest auf der ersten Ebene des Cookie-Banners klar erkennbar ist, dass auf der zweiten Ebene eine Ablehnung möglich ist und dies nicht nur aus einem unübersichtlichen Fließtext hervorgeht. Daneben berücksichtigt das Landgericht, ob eine Vielzahl von Einstellungsmöglichkeiten auf der zweiten Ebene zu einer weiteren Erschwerung der Einwilligungsverweigerung führt. Auch komme es darauf an, ob die Schaltflächen „alle Akzeptieren/Zustimmen“ oder „alle Ablehnen“ oder „Auswahl speichern“ gleichwertig positioniert und farblich so gestaltet sind, dass die Aufmerksamkeit nicht einseitig in eine Richtung gelenkt wird.

Mit diesen Erwägungen des LG München geht jedoch keine grundsätzliche Absage an eine Ausgestaltung von Cookie-Bannern mit zwei Ebenen einher, es werden allerdings hohe Anforderungen an ein Zwei-Ebenen-System gestellt, die im Einzelfall zu prüfen sind.

Im vom Landgericht München zu entscheidenden Fall wurden auf der zweiten Ebene des Cookie-Banners über 100 Auswahlmöglichkeiten angeboten, die eine informierte Einwilligung über das nachvollziehbare Maß hinaus erschwerten, wenn nicht sogar unmöglich machten.

Die grundsätzlichen Wertungen des Urteils wurden auch bei der Einschätzung der rechtmäßigen und transparenten Gestaltung von Cookie-Bannern in Angeboten der Rundfunkanstalten berücksichtigt.

Zuletzt hat das OLG Köln (Urteil vom 19.01.2024 - 6 U 80/23) ähnliche Wertungen angestellt und die Erforderlichkeit einer gleichwertigen Ablehnungsoption bekräftigt. Danach muss das Cookie-Banner so gestaltet sein, dass das Ablehnen genauso bequem wie das Akzeptieren ist.

Im konkreten Fall ging es um eine mit einem „x“ erklärte Einwilligung. Die Gestaltung eines Cookie-Banners mit dem verlinkten Button "Akzeptieren & Schließen - X" in der rechten oberen Ecke verstoße allerdings gegen die Grundsätze von Transparenz und Freiwilligkeit der Einwilligung und führe zur Unwirksamkeit der Einwilligung, da mit dem „X“-Symbol vom durchschnittlichen Nutzer lediglich das Schließen eines Fensters, nicht jedoch das Einwilligen verbunden ist. „Das "X"-Symbol ist Nutzern bekannt als Möglichkeit, um ein Fenster zu schließen, nicht aber, um in die Verwendung von Cookies und anderen Technologien durch den Websitebetreiber einzuwilligen.“[30]

[30] Rn. 68 des zitierten Urteils des OLG Köln vom 19.01.2024

Deutlich wird dadurch einmal mehr: Eine Einwilligung darf weder in missverständlicher noch in irreführender Weise eingeholt werden, sondern muss entsprechend Erwägungsgrund 42 der DSGVO durch eine Erklärung der Verarbeitungsvorgänge in verständlicher und leicht zugänglicher Form erwirkt werden, die der betroffenen Person eine echte und freie Wahl lässt.

3.4.4 Aktuelles zum Umfang des Auskunftsanspruchs

Anknüpfend an meinen letzten Tätigkeitsbericht als Rundfunkdatenschutzbeauftragter für MDR und SWR für das Jahr 2022 (Kapitel 5.5.) nehme ich den Punkt „Umfang des Auskunftsanspruchs“ erneut auf, um über die aktuelle Entwicklung in der Rechtsprechung zum Auskunftsrecht aus Art. 15 DSGVO, genauer um über die Auslegung des Rechts auf Datenkopie gemäß Art. 15 Abs. 3 DSGVO zu berichten.

Wie im letzten Tätigkeitsbericht bereits erläutert, wird eine enge sowie eine weite Auslegung des Art. 15 Abs. 3 DSGVO vertreten.

Nach der weiten Auslegung bezieht sich der Auskunfts- und auch Kopie-Anspruch auf alle vom Verantwortlichen verarbeiteten personenbezogenen Daten der betroffenen Person, das heißt, das Recht ist nicht gerichtet auf eine abstrakte Aufzählung von vorhandenen Informationen, sondern die Betroffenen haben danach einen Anspruch auf Überlassung der Informationen in der Form, wie sie dem Verantwortlichen vorliegen. Das könnte wiederum bedeuten, dass beispielsweise Schriftwechsel in der Form, wie sie beim Verantwortlichen vorhanden sind, kopiert werden müssen.

Nach der engen Auslegung wird der Auskunftsanspruch durch die bloße Angabe der Daten erfüllt, die der Verantwortliche über den Betroffenen verarbeitet. Davon umfasst sind in aller Regel die Stammdaten in unterschiedlichen Verarbeitungssituationen. Das Recht auf Kopie kann nach dieser Auffassung nicht über die personenbezogenen Daten hinausgehen, die in Artikel 15 DSGVO als Pflichtangaben festgelegt sind. Das Auskunftsrecht soll die Betroffenen in Kenntnis darüber setzen, ob und in welchem Umfang ein Verantwortlicher personenbezogene Daten verarbeitet, um sie in die Lage zu versetzen, weitere Rechte aus dem Datenschutz auszuüben. Es geht also nach dieser Auslegung vor allem um die gebotene Transparenz, dem Betroffenen das für die Durchsetzung dieses Grundrechts (informationelle Selbstbestimmung) notwendige Wissen an die Hand zu geben. Dieses Instrument kann zur Durchsetzung der Rechte aus der Datenschutz-Grundverordnung wie Berichtigung, Löschung oder Schadensersatz beitragen. Das Auskunftsrecht dient danach eben nicht der Schaffung eines Zugangs zu Verwaltungs- oder sonstigen Dokumenten, weil dies der Zielrichtung des Datenschutzrechtes nicht entspricht.

Es wird teilweise vertreten, dass ein weiter Auskunftsanspruch unter Verhältnismäßigkeitsgesichtspunkten exzessiv ist, da sich der Auskunftsersuchende in einem Rechtsstreit z. B. mit einem Arbeitgeber in eine bessere Rechtsposition zu setzen versucht. Damit würden nicht die in der DSGVO angelegten Zwecke der Rechtmäßigkeit, Kontrolle und der Transparenz verfolgt.

Die Frage zum Umfang des Anspruchs auf Datenkopie war zum Zeitpunkt des letzten Tätigkeitsberichts beim EuGH durch ein Vorabentscheidungsverfahren (Österreichische Datenschutzbehörde) platziert, aber noch nicht entschieden. Inzwischen hat sich der EuGH dazu geäußert:

Im Urteil vom 4. Mai 2023 (C-487/21) hält der EuGH fest, dass das Recht, eine „Kopie“ der personenbezogenen Daten zu erhalten, bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten zur Verfügung gestellt wird. Zum entscheidenden Begriff der Kopie erläutert der Gerichtshof, dass sich der „Begriff Kopie nicht auf ein Dokument als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen, bezieht“. Die Kopie muss daher alle personenbezogenen Daten enthalten, die Gegenstand der Verarbeitung sind.

Ein Recht, Auszüge aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u. a. diese Daten enthalten, zu erlangen, besteht nur, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die personenbezogenen Daten übermitteln zu können, wobei jedoch auch die Rechte und Freiheiten anderer Personen zu berücksichtigen sind (vgl. Art. 15 Abs. 4 DSGVO), um etwaige Konflikte aufzulösen.

Aus dieser Wertung wird einerseits deutlich, dass einer effektiven Ausübung des Auskunftsrechts hohes Gewicht eingeräumt wird. Es soll sichergestellt werden, dass betroffene Personen präzise, leicht zugängliche und verständliche Informationen über die Verarbeitung ihrer personenbezogenen Daten erhalten können. Andererseits aber stellt eine Kopie von Dokumenten eher den Ausnahmefall dar, da sich der Begriff Kopie, wie dargestellt, lediglich auf die personenbezogenen Daten bezieht. Im Übrigen stellt der Gerichtshof - beruhend auf dieser Auslegung - klar, dass sich der im Sinne des Art. 15 Abs. 3 Satz 3 DSGVO verwendete Begriff „Informationen“ ausschließlich auf personenbezogene Daten bezieht, von denen der für die Verarbeitung Verantwortliche gemäß Satz 1 dieses Absatzes eine Kopie zur Verfügung stellen muss.

Festgehalten werden kann, dass sich der EuGH[31] damit für einen Mittelweg zwischen enger und weiter Auslegung des Auskunftsanspruchs in Form der Datenkopie gemäß Art. 15 Abs. 3 DSGVO entschieden hat und im Einzelfall eine sorgfältige Abwägung zwischen den Rechten betroffener Personen und den Rechten und Freiheiten anderer, wie Geschäftsgeheimnissen oder geistigem Eigentum, erfolgen muss. Der Begriff „Kopie“ ist im Ergebnis nicht wörtlich zu verstehen, sondern im Sinne der Ziele der DSGVO ausschließlich bezogen auf personenbezogene Daten auszulegen und damit Betroffenen die Rechtmäßigkeit der Verarbeitung ihrer Daten nachvollziehbar zu machen.

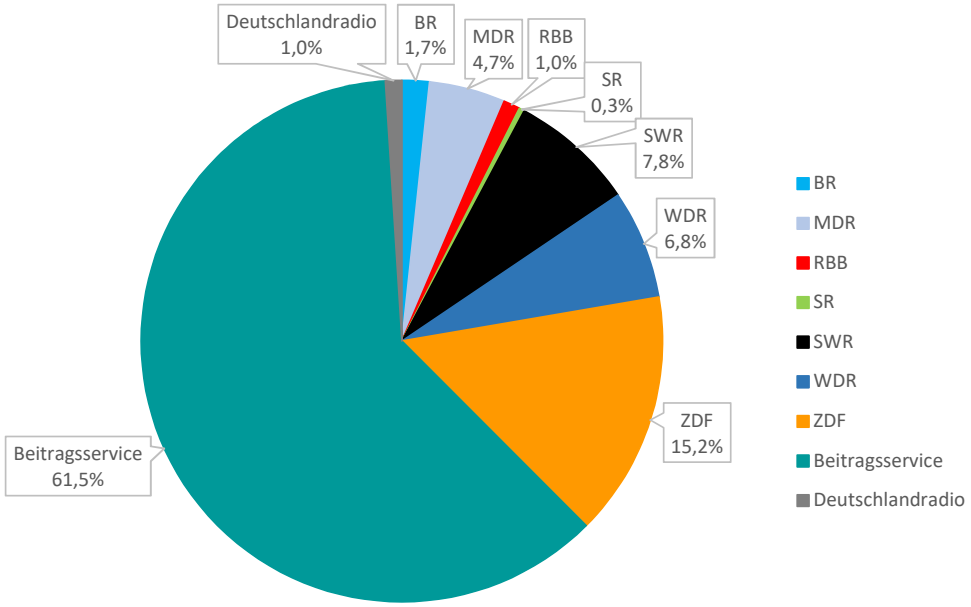
4 Eingaben beim Rundfunkdatenschutzbeauftragten

Der Rundfunkdatenschutzbeauftragte ist zuständig für die Bearbeitung von Beschwerden. Nach § 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, § 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 durch Art. 77 DSGVO gewährleistet.

[31] Der EuGH hat diese Auslegung des Rechts auf Datenkopie bereits in einem weiteren Urteil zur Patientenakte bestätigt - EuGH, Urteil vom 26.10.2023 - C 307/22.

4.1 Eingaben gesamt

Im Jahr 2023 erreichten die Aufsichtsbehörde 296 Eingaben, die sich in Beschwerden und Sonstige Anfragen unterteilen.

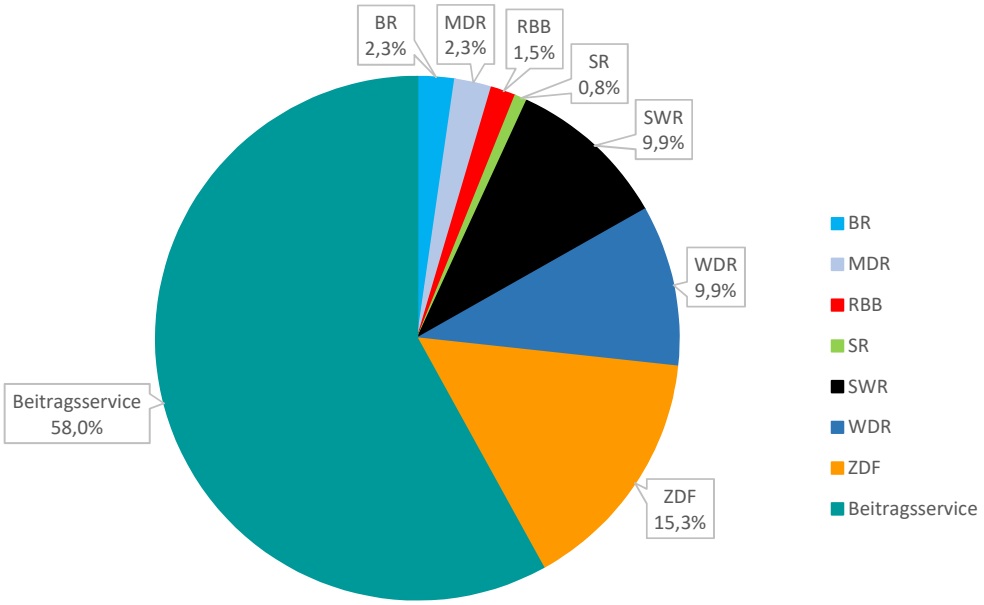


Auf die Rundfunkastalten bezogen verteilen sich diese wie folgt:

Eingaben gesamt	Anzahl	Prozent
Beitragsservice	**182**	61,5%
BR	**5**	1,7%
Deutschlandradio	**3**	1,0%
MDR	**14**	4,7%
RBB	**3**	1,0%
SR	**1**	0,3%
SWR	**23**	7,8%
WDR	**20**	6,8%
ZDF	**45**	15,2%
Gesamt	**296**	100%

4.2 Beschwerden

Unter den 296 Eingaben befanden sich in 131 Beschwerden (44 %), von diesen Beschwerden waren 21 begründet und mit datenschutzrechtlichem Bezug (16%).

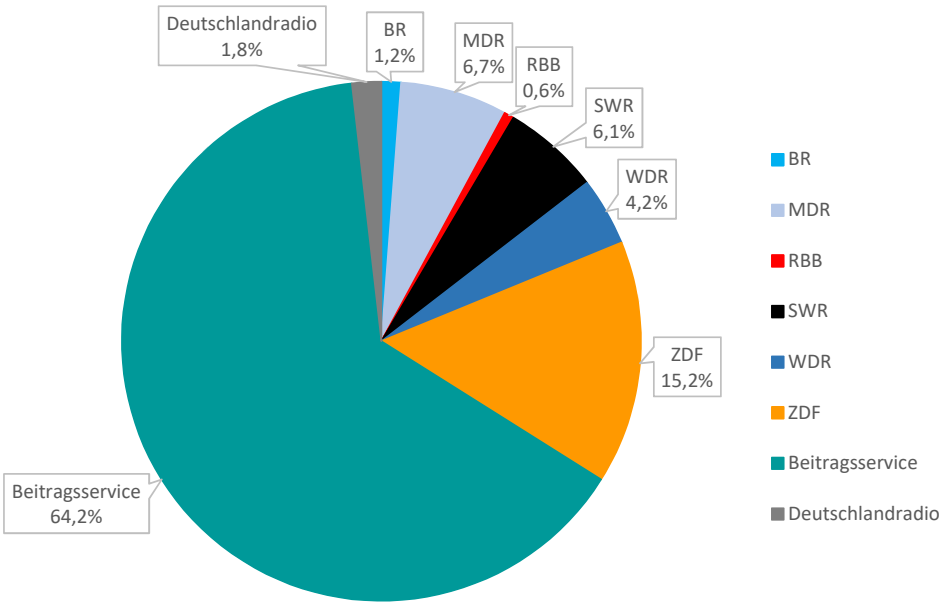


Auf die Rundfunkanstalten bezogen verteilen sich diese wie folgt:

Beschwerden	(begründet)	Anzahl	Prozent
Beitragsservice	(9)	**76**	58,0%
BR	(0)	**3**	2,3%
Deutschlandradio	(0)	**0**	0,0%
MDR	(1)	**3**	2,3%
RBB	(1)	**2**	1,5%
SR	(0)	**1**	0,8%
SWR	(1)	**13**	9,9%
WDR	(7)	**13**	9,9%
ZDF	(2)	**20**	15,3%
Gesamt	(21)	**131**	100%

4.3 Sonstige Anfragen

Unter den 296 Eingaben befanden sich 165 Sonstige Anfragen (46 %). Unter diesen summieren sich Zuschriften, die von vermeintlichen Datenschutzthemen und fehlgeleiteten Auskunftsersuchen über in der Zuständigkeit einer anderen Behörde liegende Eingaben bis hin zu spezifischen Anfragen oder Beschwerden zum Beitragseinzug reichen.



Auf die Rundfunkanstalten bezogen verteilen sich diese wie folgt:

Sonstige Anfragen	Anzahl	Prozent
Beitragsservice	**106**	64,2%
BR	**2**	1,2%
Deutschlandradio	**3**	1,8%
MDR	**11**	6,7%
RBB	**1**	0,6%
SR	**0**	0,0%
SWR	**10**	6,1%
WDR	**7**	4,2%
ZDF	**25**	15,2%
Gesamt	**165**	100%

4.4 Dienstaufsichtsbeschwerde

Im Berichtsjahr wurde eine Dienstaufsichtsbeschwerde gegen mich erhoben. Eingang in diesen Bericht findet dies aus Transparenzgründen, aber auch weil ein grundsätzliches Thema berührt ist.

Im Wesentlichen ging es um die Frage, ob der Rundfunkdatenschutzbeauftragte verpflichtet ist, Beschwerdesachverhalte von betroffenen Personen auch telefonisch entgegenzunehmen und diese ggf. zu diskutieren.

Der hier gegenständliche Fall ist insoweit zwar nicht repräsentativ, da mit großer Vehemenz bei meinem Sekretariat ein Gespräch mit mir eingefordert wurde, ohne den Anlass oder einen sonstigen Grund für einen solchen Austausch zu nennen. Die Angelegenheit endete damit, dass mein Büro einen Tag lang einem regelrechten Telefonterror ausgesetzt war. Der Petent hat sich daraufhin beim Verwaltungsrat des Westdeutschen Rundfunks beschwert, woraufhin ich eine ausführliche Stellungnahme abgegeben habe:

Im Sinne einer ordnungsgemäßen Bearbeitung eines Anliegens ist es nach meiner Überzeugung stets sinnvoll, die Beschwerde oder das Anliegen schriftlich zu formulieren und an den Rundfunkdatenschutzbeauftragten zu senden. Ansonsten scheint eine ordnungsgemäße Beschwerdebearbeitung kaum möglich. Aus diesem Grund erkenne ich kein grundsätzliches Recht, mit mir als Behördenleiter zu sprechen. Sollte es sich aufgrund von besonderen Umständen anbieten, mit Beschwerdeführer oder Petenten zu führen, so bin ich dazu stets gern bereit. Dies ist abzugrenzen von einem telefonischen Erstkontakt, in dem oftmals auch - so zumindest meine Erfahrung aus der Vergangenheit - sehr emotional und wenig sachlich argumentiert wird.

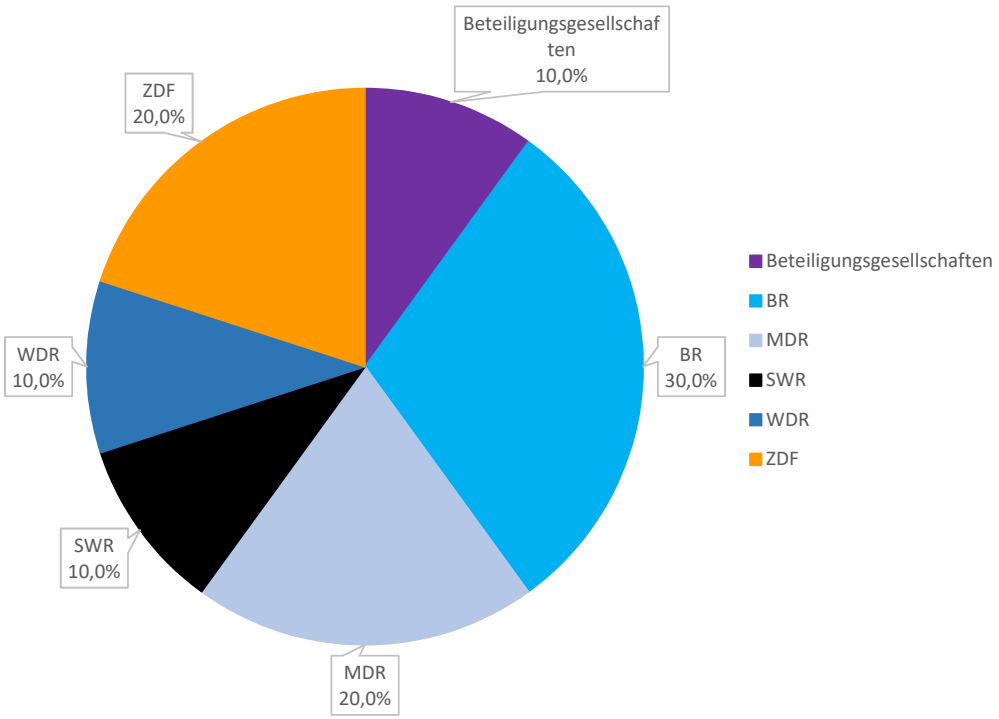
Im Ergebnis hat der Verwaltungsrat des WDR der Beschwerde nicht stattgegeben und mir bestätigt, mich korrekt und im Einklang mit den geltenden Regelungen verhalten zu haben.

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 zu unbefugten Offenlegung von personenbezogenen Daten führt (Artikel 4 Ziffer 12 DSGVO), ist gemäß Artikel 33 DSGVO die Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung zu informieren. Führt diese 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 Artikel 34 DSGVO vorgeschriebenen Benachrichtigung davon betroffener Personen vorliegen. Aus Gründen der Risikominimierung ist anzuraten, im Zweifel die Aufsichtsbehörde zu unterrichten.

Zehn Meldungen zu Datenschutzvorfällen in Rundfunkanstalten und Beteiligungsgesellschaften gingen in der Aufsichtsbehörde ein.



Die Meldungen verteilen sich wie folgt:

Datenschutzvorfälle	Anzahl	Prozent
Beitragsservice	**0**	0,0%
Beteiligungsgesellschaften	**1**	10,0%
BR	**3**	30,0%
Deutschlandradio	**0**	0,0%
MDR	**2**	20,0%
RBB	**0**	0,0%
SR	**0**	0,0%
SWR	**1**	10,0%
WDR	**1**	10,0%
ZDF	**2**	20,0%
Gesamt	**10**	100%

6 Schwerpunktthemen des Rundfunkdatenschutzbeauftragten

Beim Verfassen dieses Berichts hatte ich mich zu fragen, über welche Themen ich berichten möchte. 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. Davon ausgehend habe ich die folgende Auswahl getroffen und denke, dass sie einen guten Überblick ermöglicht, der sowohl die Arbeit an einzelnen Themen als auch Beschäftigung mit übergeordneten Problematiken angemessen beleuchtet.

6.1 Nutzungsmessung

Das Audit zur Nutzungsmessung, über das nachfolgend im Kapitel 6.1.2 Audit der Nutzungsmessung in den Online-Angeboten der Rundfunkanstaltenberichtet wird, hat aufschlussreiche Erkenntnisse geliefert und gezeigt, dass dieses Thema datenschutzrechtlich nach wie vor schwierig und im Detail nicht unumstritten ist.

6.1.1 Zulässigkeit der Nutzungsmessung

Ich hatte mich insoweit immer wieder mit Fragen und Vorwürfen auseinanderzusetzen, der öffentlich-rechtliche Rundfunk würde Nutzungsmessungen vornehmen, ohne erforderliche Einwilligungen einzuholen.

Grundsätzlich gilt (siehe auch Kapitel 4.3. meines Tätigkeitsberichtes zum Jahr 2023 (MDR und SWR) sowie Tätigkeitsbericht von Herrn Binder zum Jahr 2020, Rn. 104 ff.), dass eine statistische und anonymisierte Nutzungsmessung (in Ansehung der gewonnenen Ergebnisse) durch die Rundfunkanstalten auch ohne Einwilligung der Nutzerinnen und Nutzer möglich ist, da sie sich eben nicht auf eine einzelne Person bezieht, sondern auf grundlegende Nutzungs- und Erfolgsdaten. Die Argumentation stützt sich im Wesentlichen auf den verfassungsrechtlichen Auftrag der öffentlich-rechtlichen Rundfunkanstalten und die daraus abgeleitete Verpflichtung, eine zeitgemäße Gestaltung der Telemedienangebote für alle Bevölkerungsgruppen sicherzustellen (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 auch Auswirkungen auf die Akzeptanz der Bevölkerung aufweisen. Insofern lässt sich gut begründen, dass dies zum Auftrag gehört, weshalb eine Einwilligung in solcherlei Nutzungsmessung nicht erforderlich ist.

Daher fällt es teilweise aber schwer nachzuvollziehen, dass in der Tat zumindest kurzzeitig personenbezogene Daten (etwa die IP-Adresse) verarbeitet werden. Diese werden jedoch nach unserem aktuellen Kenntnisstand durch die Dienstleister nach den entsprechenden Maßgaben sofort anonymisiert, sodass im Messungsergebnis kein Personenbezug mehr zu finden ist. Es ergeben sich hier allerdings relevante Detailfragen hinsichtlich der Anonymisierungsmethoden. Diese zu klären und die richtigen Impulse zu setzen, hat sich das Audit zur Aufgabe gestellt.

Gewiss kann man bei der rechtlichen Würdigung anderer Meinung sein, aber in Ansehung des verfassungsrechtlichen Auftrags und der besonderen Stellung des öffentlich-rechtlichen Rundfunks halte ich dieses Ergebnis der Einwilligungsfreiheit nach wie vor für richtig und sachgerecht. Wünschenswert wäre in der Tat eine klarere Regelung, die insbesondere die statistische Nutzungsmessung einem besonderen und vielleicht vereinfachten Regime unterwirft. Die französische Aufsichtsbehörde CNIL[32] hat diesen Weg teilweise beschritten und ein Tool, das auch vom öffentlich-rechtlichen Rundfunk eingesetzt wird, einwilligungsfrei gestellt, da tatsächlich nur statistische Daten erzeugt werden und die Datenverarbeitung insofern nicht das Ziel verfolgt, einzelne Nutzer gläsern und wiederauffindbar zu machen. Dies halte ich im Ergebnis für richtig, allerdings ist es dem europäischen Gesetzgeber vorbehalten, hier eine einheitliche Regelung zu finden: Die angestrebte EU Privacy Verordnung wäre hier die richtige Stelle, um eine solche Regelung zu treffen.

6.1.2 Audit der Nutzungsmessung in den Online-Angeboten der Rundfunkanstalten

Durch die insbesondere durch die kommerziellen Angebote anderer Anbieter eingesetzten Einwilligungsbanner im Hinblick auf Cookies und Nutzungsmessung haben mich oft Fragen und auch Beschwerden dazu erreicht, warum der öffentlich-rechtliche Rundfunk hier eine andere Praxis verfolgt. Aufgrund dessen habe ich mich entschieden, mir einen Gesamteindruck über alle Nutzungsmessungsaktivitäten in den Rundfunkanstalten zu verschaffen, zunächst nur als Datengrundlage, um dann die richtigen Schlüsse im Hinblick darauf zu ziehen, ob die eingesetzten Nutzungsmessungsverfahren auch tatsächlich den datenschutzrechtlich gebotenen Anforderungen und dem soeben erläuterten öffentlich-rechtlichen Auftrag entsprechen. Die beschriebene Auftragserfüllung bedeutet nämlich nicht, dass in jeglicher Tiefe und mit jeglichem Anbieter und damit mit jedem eingesetzten Tool ohne weitere Prüfung die Nutzung in den Angeboten gemessen werden darf. Daher habe ich einen Fragebogen entwickelt, den ich den betrieblichen Datenschutzbeauftragten zur Kenntnis gegeben und den Rundfunkanstalten zur Beantwortung zugesandt habe.

[32] https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-daudience

Der Fragenkatalog verfolgt zunächst die Absicht, sämtliche Angebote wie Websites, Apps, Social Media Angebote und HbbTV der Rundfunkanstalten zu erfassen, sowie die dabei eingesetzte Messmethode. Erfragt wurden Zweck und Ziel der Messungen, die genaue inhaltliche und technische Beschreibung der Messmethoden, die vertragliche Anbindung der Dienstleister, ebenso die Rechtslage im Hinblick auf den Datenschutz, auch mit Blick auf das TTDSG. Zudem wurden Informationen abgefordert zur eingesetzten Anonymisierung und zur Verhinderung der Wiederherstellbarkeit des Personenbezugs. Wichtig und damit von Interesse ist auch, dass auf die Nutzungsmessung transparent hingewiesen und die datenschutzrechtlichen Besonderheiten so erläutert werden, damit sie leicht zu verstehen und nachvollziehbar sind.

Die Rückläufe haben ein sehr unterschiedliches und vielfältiges Bild ergeben und diverse Nachfragen erfordert. Das Ergebnis des Audits lag zum Ende des Berichtsjahres damit noch nicht vor. Gesagt werden kann jedoch bereits Folgendes:

Ein Großteil der verwendeten Tools wird 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 ohne Einwilligung eingesetzt. Ob sich alle Tools, die von Rundfunkanstalten genutzt werden, auch tatsächlich unter die hohen Maßstäbe dieser Rechtsgrundlage fassen lassen, wird 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 hohen Bedeutung dieses Tools haben wir daraufhin eine Prüfung der Anonymisierungsmethode von Piano begonnen. Im Zuge dessen erkennen wir Anlass für eine vertiefte Prüfung hinsichtlich der konkreten Datenverarbeitungen und Anonymisierungen bei diesem Dienstleister. Dies muss genau und kritisch in den Blick genommen werden; ein Ergebnis lag zum Redaktionsschluss noch nicht vor. Im nächsten Bericht werde ich darüber informieren.

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 und 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 Analysen von Drittplattformen genutzt werden. Ob und mit welcher Konsequenz für eine rechtmäßige Nutzung wir diese Einschätzung teilen, ist auch Gegenstand der zurzeit noch stattfindenden Auswertung der Informationen und deren Prüfung.

Auch die Antworten auf unsere Nachfragen waren von unterschiedlicher Qualität, so wurden wir teilweise an die Dienstleister verwiesen, um Unklarheiten zu klären, was jedoch Aufgabe des Verantwortlichen gewesen wäre.

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

Fazit: Eine so ausführliche Befassung mit dem Thema hat sich - so viel kann bereits festgestellt werden - als ertragreich und sinnvoll erwiesen, da sie einen Blick auf die unterschiedliche Handhabung in den Rundfunkanstalten ermöglicht. Dies ist grundsätzlich nicht zu beanstanden, muss jedoch im Hinblick auf die datenschutzrechtliche Zulässigkeit genau in den Blick genommen werden. Aufgabe als Aufsichtsbehörde ist daher zunächst, auf die Unterschiede hinzuweisen, noch einmal für das Thema zu sensibilisieren und stichprobenartig vertieft zu prüfen.

Aus meiner Sicht sind zwei Dinge entscheidend: Erstens ist die Frage zu stellen nach dem Sinn und Zweck der Nutzungsmessung und den damit gewonnenen Daten und Erkenntnissen. Zweitens muss der Blick gerichtet werden auf die von den Rundfunkanstalten eingebundenen Unternehmen. Die bisher möglichen Auswertungen haben gezeigt, dass teilweise nicht in der gebotenen Tiefe Klarheit darüber herrscht, welcherlei Daten genau bei den Dienstleistern verarbeitet werden. Hier - so zeigt es sich wieder einmal - kann man sich nicht nur auf die vertraglichen Grundlagen verlassen, sondern muss konkret mit den Dienstleitern in den Austausch treten.

Über die Ergebnisse dieses Audit wird im nächsten Tätigkeitsbericht eingehend berichtet werden.

6.1.3 Web-Compliance der Nutzungsmessung

Ein Software-Unternehmen ist im September 2023 auf mich zugekommen, da es eine Analyse der Web-Compliance der Websites der Rundfunkanstalten um Hinblick auf TTDSG und DSGVO ins Auge gefasst hatte.

Vor dem Hintergrund der medialen Aufmerksamkeit, die mit einer ähnlich gelagerten Prüfung der Websites der Bundesregierung durch eine Veröffentlichung dieser Ergebnisse auf der Website Business-Insider erreicht wurde, habe ich den Kontakt mit dem Unternehmen aufgenommen. Dies war auch deshalb von besonderem Interesse, da zum Zeitpunkt der Kontaktaufnahme meine umfassende Untersuchung der Nutzungsmessungs-Tools in den Angeboten der Rundfunkanstalten lief (siehe dazu Kapitel 6.1.2).

In einem Telefonat habe ich die Besonderheiten erläutert, die den öffentlich-rechtlichen Rundfunk sowie die dabei zu berücksichtigenden datenschutzrechtlichen Ausnahmeregelungen betreffen. Ich bin dabei auf das Medienprivileg und den Auftrag des öffentlich-rechtlichen Rundfunks eingegangen. Vor dem Gespräch waren mir bereits Ausschnitte von Prüfungsergebnissen einzelner Websites der Rundfunkanstalten zur Veranschaulichung zur Verfügung gestellt worden. Dabei wurde deutlich, dass die genannten Besonderheiten des öffentlich-rechtlichen Rundfunks bisher keine Rolle bei der Untersuchung spielten und damit ein verzerrtes Bild der Datenschutzkonformität zeigten. Insofern habe ich den Austausch als gewinnbringend angesehen, einerseits, um seitens der verantwortlichen Rundfunkanstalten Lücken in punkto Transparenz durch diese verwendeten Tools erkennbar zu machen und zukünftig zu schließen, und andererseits, um eine Veröffentlichung zu vermeiden, die ein falsches Bild der Rundfunkanstalten insbesondere bei der Nutzungsmessung zeigt. Mit den betrieblichen Datenschutzbeauftragten der Rundfunkanstalten habe ich die Thematik in der Folge des Gesprächs erörtert.

Ich halte einen weiteren Austausch mit dem Anbieter auch perspektivisch für möglich und ggf. hilfreich.

6.1.4 Umstellung Cookie-Banner ZDF

Mit dem ZDF wurde die Frage erörtert, ob das Cookie-Einwilligungsbanner auf der Website zdf.de angesichts der aktuellen Rechtsprechung (siehe hierzu Kapitel 3.4.3) angepasst werden sollte oder gar muss. Unter Hinweis auf Kapitel 6.8.3, in dem die grundlegenden Problematik genauer erläutert wird, kann ich an dieser Stelle darüber berichten, dass in das Einwilligungsbanner des ZDF auf erster Ebene eine grundlegende Funktion integriert wurde, die es den Nutzenden ermöglicht, bereits zu diesem Zeitpunkt sämtliche zustimmungsbedürftige Datenverarbeitungen abzulehnen, ohne auf einer zweiten Ebene eine Auswahl treffen zu müssen. Dies ist im Sinne der Nutzerfreundlichkeit, aber auch im Hinblick auf die Freiwilligkeit einer solchen Entscheidung zu begrüßen. Bei dieser Anpassung wurde ebenso berücksichtigt, dass eine Interaktion mit dem Einwilligungsbanner erforderlich ist, bevor man die Angebote des ZDF nutzen kann, weshalb eine unmittelbare Ablehn-Möglichkeit gefordert wurde.

Auf der zweiten Ebene kann der interessierte Nutzende auf Wunsch seine Einstellungen individuell anpassen. Die erforderlichen technischen Cookies und die aus Sicht des öffentlich-rechtlichen Rundfunks erforderliche Erfolgsmessung sind immer aktiv und können somit auch nicht ausgeschaltet werden, was datenschutzrechtlich in Ordnung ist. Die Nutzenden können allerdings entscheiden, ob sie eine Personalisierung des Angebotes wünschen und zudem Social Media und externe Drittsysteme einschalten wollen. Da bereits auf der ersten Ebene des Einwilligungsbanners die Möglichkeit gegeben wird, auch diese Funktionen abzulehnen, begegnet eine

Anpassungsmöglichkeit auf der Folge-Ebene des Einwilligungsbanners keinen rechtlichen Bedenken. Auch hat das ZDF noch Anpassungen hinsichtlich der Platzierung der jeweiligen Buttons vorgenommen, um möglichst transparent zu informieren und eine einfache Handhabung zu gewährleisten. Das somit gewonnene Ergebnis halte ich für gelungen und freue mich, dass in diesem Zusammenhang der Austausch zwischen dem ZDF und dem Rundfunkdatenschutzbeauftragten in solcherlei Ergebnis münden konnte.

6.2 Künstliche Intelligenz

An verschiedenen Stellen in diesem Bericht ist das Thema KI bereits angeklungen. Es ist fast schon unnötig zu sagen, dass im Berichtsjahr und mit an Sicherheit grenzender Wahrscheinlichkeit in den Folgejahren das Thema Künstliche Intelligenz und entsprechende Algorithmen eine große Rolle in der Realität der Rundfunkanstalten spielen werden. Nicht umsonst wird dieses Thema auch in der Öffentlichkeit als technologischer Umbruch und weiterer Meilenstein in der IT-Anwendung wahrgenommen. Nicht zuletzt durch KI-Anwendungen, die auch in den Alltag Einzug gehalten haben (z.B. Chat GPT), ist es ein Thema, das sprichwörtlich in aller Munde ist. Zur in diesem Zusammenhang wichtigen KI-Verordnung verweise ich auf Kapitel 3.1.5 Artificial Intelligence Act (AIA) / KI-Verordnung (KI-VO) dieses Berichts.

Auch meine Aufsichtsbehörde hat sich gemeinsam mit der RDSK entschlossen, ungeachtet der starken dynamischen Entwicklung und der sich ständig ändernden Rahmenbedingungen erste Einschätzungen und Orientierungen hinsichtlich des Einsatzes von Künstlicher Intelligenz in den Rundfunkanstalten unter Berücksichtigung des Datenschutzes zu verfassen. In Folge dessen wurde bereits im August 2023 eine Orientierungshilfe fertiggestellt (siehe dazu Kapitel 7.2.3), die erste Eckpunkte und datenschutzrechtliche Anknüpfungspunkte hinsichtlich des Einsatzes von Künstlicher Intelligenz (insbesondere zunächst zur Erprobung) bieten soll. An dieser Stelle weise ich darauf hin, dass dieses Papier als interne Orientierungshilfe gedacht ist, die aufgrund der schnellen Fortentwicklung lediglich einen vorläufigen Charakter hat und deswegen nicht veröffentlicht worden ist. Dies hat die RDSK gemeinsam entschieden, sodass ich an dieser Stelle lediglich die wesentlichen Inhalte und Schwerpunkte dieser Orientierungshilfe wiedergebe.

Wie immer bei Anwendungen, in denen personenbezogene Daten verarbeitet werden, muss 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 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, eine Rechtsgrundlage für die konkrete Verarbeitung zu finden, wie sie in Art. 6 Abs. 1 DSGVO vorgegeben sind. Eine Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO ist immer zusätzlich dann erforderlich, wenn besondere und hohe Risiken für die Rechte und Freiheiten der betroffenen Personen zu befürchten sind.

Risiken beim Einsatz von KI, wie z.B. mangelnde oder gar fehlende Transparenz im Hinblick auf die mit der KI verbundene Datenverarbeitung sind zu prüfen, ebenso ist die Erfüllung der Informationspflichten gegenüber den betroffenen Personen sicherzustellen, was sich im Einzelfall als schwierig erweisen kann. Ebenso ist zu beachten, dass die Betroffenenrechte wie Auskunft- oder Löschungsersuchen erfüllt werden können müssen. Schließlich muss die Frage gestellt werden, wo die Datenverarbeitung stattfindet.

Ein Schwerpunkt war das Problem, welche Verantwortungssphären sich beim Einsatz von KI ergeben: Kann eine Auftragsverarbeitung angenommen werden, muss 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 behält. 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 Folgendes zu beachten:

Anwendungen können redaktionelles Arbeitsmittel und/oder Berichtsgegenstand sein. Die eingesetzten Systeme dürfen die Einhaltung des Datengeheimnisses nicht gefährden und den Grundsatz der Vertraulichkeit und Integrität zur Gewährleistung der Datensicherheit nicht verletzen. Die in die 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 wahren 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 diese Anwendungen 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). 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).

Die Verantwortlichen sind aufgerufen, einen Evaluierungsprozess einzuführen, um den Einsatz von KI überprüfbar zu machen.

6.3 Medienprivileg

Das Medienprivileg bezeichnet die Bereichsausnahme für die insoweit privilegierten Medien von den datenschutzrechtlichen Anforderungen. 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 das öffentliche Informationsinteresse, die Freiheit von Presse und Rundfunk (Art. 5 GG) und damit das Veröffentlichungsinteresse in den Vordergrund. Datenschutz hingegen wird eher restriktiv gehandhabt, es besteht ein sogenanntes Verbot mit Erlaubnisvorbehalt, was nichts Anderes besagt, als dass es für jede Datenverarbeitung (außerhalb des medienprivilegierten Bereichs) eine explizite Rechtsgrundlage braucht.

6.3.1 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 gewährleistet werden.

Entscheidend für die Anwendung des Medienprivilegs ist also die Einordnung der Datenverarbeitung unter den Begriff „journalistische Zwecke“[33]. 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 einen Beitrag zur öffentlichen Meinungsbildung leisten, 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 Personaldatenverarbeitung, 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 der Bedingungen des Art. 6 DSGVO erfüllt sein.

Für die Datenverarbeitung im journalistischen und redaktionellen Kontext in den Rundfunkanstalten greift somit das Medienprivileg. 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. Nachfolgend werden bestimmte Grenzbereiche, die mich im Kontext des Rundfunkdatenschutzes befasst haben, identifiziert und definiert, damit letztlich eine rechtssichere Datenverarbeitung in diesen Bereichen erfolgen kann.

6.3.2 Reichweite des Medienprivilegs im Rahmen von Programmbeschwerden

In meiner Aufsichtspraxis hatte ich mich im Rahmen einer Beschwerde mit der Frage zu befassen, ob eine Programmbeschwerde zu Klärungszwecken an eine Dritte, im gegenständlichen Beitrag bereits zu Wort gekommene Expertin, weitergegeben werden durfte und ob auf diesen Fall die medienrechtliche Privilegierung Anwendung finden kann. Ich hatte mich also damit zu beschäftigen,

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

ob die inhaltliche Überprüfung von Programmbeschwerden zugrunde liegenden journalistischen Beiträgen zum Kernbereich der journalistischen Tätigkeit zählen.

Programmbeschwerden, die eine Verletzung von Programmgrundsätzen behaupten und sich auf das konkrete Programm beziehen, knüpfen unmittelbar an die journalistisch hergestellten Inhalte an und tangieren damit das Medienprivileg. Es war daher die Frage zu beantworten, ob auch die Auseinandersetzung mit der Programmbeschwerde innerhalb der Rundfunkanstalt noch unter das Medienprivileg subsumiert werden kann. Da zum vom Medienprivileg geschützten Bereich auch die Recherche, Redaktionsarbeit, Veröffentlichung, Dokumentation und auch Archivierung personenbezogener Daten zu publizistischen Zwecken gehören (vgl. BGH Urteil vom 01.02.2011 – VI ZR 345/09), ist die Anwendung beim Umgang mit Programmbeschwerden zumindest nicht abwegig. Man könnte einwenden, dass das Merkmal der Zielrichtung einer Veröffentlichung für einen unbestimmten Personenkreis damit ggf. nicht mehr erfüllt sein könnte; dem ist aber entgegenzuhalten, dass die Veränderung oder Berichtigung von journalistischen Arbeiten/Inhalten als Folge der Auseinandersetzung mit solchen Programmbeschwerden möglich ist. Zudem fließen die Erkenntnisse aus einer Programmbeschwerde ggf. in zukünftige Produktionen ein oder führen zu Korrekturen, die auch wiederum publizistisch relevant sein könnten (bspw. Gegendarstellungen).

Die Definition und auch die Rechtsgrundlage des Medienprivilegs lässt pauschale Charakterisierungen von bestimmten Tätigkeiten als vom Medienprivileg gedeckt oder nicht gedeckt kaum zu. Vielmehr muss eine Einstufung am Einzelfall vorgenommen werden, um der im Hintergrund mit dem Medienprivileg anzustellenden ausdifferenzierten Abwägung zwischen informationeller Selbstbestimmung und Pressefreiheit gerecht zu werden.

Das spricht dafür, im Einzelfall bei klarem Programmbezug die Einschlägigkeit des Medienprivilegs anzunehmen.

Ich habe mich von der Überlegung leiten lassen, dass investigative oder journalistische Arbeit häufig auf einem Stock gesammelter Erkenntnisse und immer weiter angereichertem Wissen beruht. Sie ist nicht vereinbar mit der Vorstellung eines immer nur kurzen Projektbezugs, nach dessen „Erledigung“ die Daten gelöscht werden müssen. Auch gilt, dass die Datenverarbeitung nicht nur für die klassische journalistische Recherche privilegiert ist. Eine Datenübermittlung, die ohne einen von vornhinein definierten oder erkennbaren Zusammenhang mit einer redaktionellen Zielsetzung stattfindet, ist unter den Schutzbereich des Medienprivilegs zu fassen, wenn sie journalistischen Zwecken dienen soll. Das Medienprivileg darf aber ebenso wenig vorgeschoben werden, wenn eigentlich ein anderer Zweck verfolgt wird. Dies war hier nicht der Fall, denn die Bearbeitung von einer - wie in diesem Fall - eng mit der journalistischen Tätigkeit verbundenen Beschwerde, verfolgte keinen anderweitigen Zweck. Diesem Ergebnis steht nicht entgegen, dass mit der Weiterleitung der

Daten auch Erkenntnisse für die Bearbeitung der Beschwerde gewonnen werden konnten, denn die Beschwerde bezog sich unmittelbar auf die veröffentlichten Inhalte.

Die Abgrenzung ist nicht immer einfach und im Zweifel muss es heißen: Das Medienprivileg kann nur dort angewendet werden, wo wirklich journalistische Bereiche betroffen sind, denn der Schutzbereich des Datenschutzes darf nicht leichtfertig eingeengt oder gar vernachlässigt werden.

Im konkreten Fall habe ich entschieden, dass die Datenweitergabe dem Medienprivileg unterfiel, weil nachvollziehbar war, dass die Redaktion mit der Datenweitergabe an eine externe Expertin ihr Wissen erweitern und für zukünftige redaktionelle Zwecke verwenden wollte. Die Programmbeschwerde war somit als Anstoß und Motivation für diese journalistische Datenverarbeitung zu werten.

6.3.3 Reichweite des Medienprivilegs bei Recherche von Privatpersonen

Ein weiterer Grenzbereich, der mir im Jahr 2023 im Zuge von Beschwerden begegnet ist, war die Frage, ob das Medienprivileg auch für Recherche von Privatpersonen gilt, die diese mit dem Zweck die Presse zu informieren durchführen.

Wie der EuGH bereits in der Rechtssache Satamedia[34] entschieden hat, sind die Abweichungen und Ausnahmen des Datenschutzrechts durch das Medienprivileg nicht nur auf Medienunternehmen anwendbar, sondern auf jeden, der journalistisch tätig ist[35]. Dabei soll es für die Privilegierung auch nicht auf eine berufliche Tätigkeit ankommen, sondern auch jede Art von öffentlichkeitswirksamer Verbreitung - linear oder nichtlinear - im Wege der Netzkommunikation erfasst sein, wie zum Beispiel Blogs.[36] Erforderlich ist jedoch der klare Bezug zur Öffentlichkeit (Zielrichtung = unbestimmter Personenkreis), um von der nicht erfassten Individualkommunikation[37] oder auch der Kommunikation in privaten Gruppen eines Messenger-Dienstes abzugrenzen.

Der Erwägungsgrund 153 zur DSGVO gibt in Satz 7 ausdrücklich vor, dass der Begriff „Journalismus“ weit ausgelegt werden muss, „um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen“. Auch daraus kann bereits geschlussfolgert

[34] EuGH EuZW 2009, 108, Rn. 60 – Satamedia; EuGH, Urt. v. 14.02.2019 – C 345/17, Rn. 57 – Buivids
[35] Zu diesem Zeitpunkt noch die Vorgängerregelung des Art. 85 Abs. 2 DSGVO betreffend (Art. 9 DSRL); Bienemann, in: Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, DS GVO Art. 85 Rn. 19
[36] Specht/Bienemann, in: Sydow, Europäische Datenschutz-Grundverordnung, 2. Aufl. 2018, Rn. 15; Koreng/Feldmann ZD 2012, 311 (314)
[37] Cornils, in: BeckOK InfoMedienR, 41. Ed. 1.2.2021, DS-GVO Art. 85, Rn. 70

werden, dass nicht nur klassische Presseorgane, sondern auch die Recherchetätigkeiten von Personen, die beruflich nicht in erster Linie als Journalist tätig sind, privilegiert sein können.

Trotz dieser Vorgabe zur weiten Auslegung ist der Begriff nicht uferlos und wird ebenfalls durch Erwägungsgrund 153 DSGVO in Satz 2 eingegrenzt, wonach Abweichungen und Ausnahmen von der DSGVO nur dann gelten sollen, wenn eine Datenverarbeitung ausschließlich zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt.[38] Sobald daher ein weiterer Zweck erkennbar ist , unterliegt die Datenverarbeitung insgesamt den Bestimmungen der DSGVO und würde nicht vom Medienprivileg umfasst werden (siehe für Beispiele für Ausnahmen vom Anwendungsbereich Kapitel 6.3.1). Abweichende Spielräume des nationalen Gesetzgebers für eine privilegierte Verarbeitung personenbezogener Daten sind dann nicht mehr eröffnet.[39] Weitere eingrenzend wirkende auch qualitative Anforderungen oder eine bestimmte Häufigkeit oder Regelmäßigkeit der Publikationstätigkeit lassen sich mit der offenen Auslegung der DSGVO sowie der EuGH-Rechtsprechung nicht vereinbaren. Journalistischen Sorgfaltsstandards dürfen kein Kriterium für die datenschutzrechtliche Einordnung sein. Damit fallen auch nur gelegentliche kommunikative Aktivitäten als Leserbriefschreiber oder in Netzforen unter die Journalismus-Kategorie im datenschutzrechtlichen Sinn.[40] Hier gilt jedoch die von BGH[41] und EuGH[42] etablierte Formel, dass die meinungsbildende Wirkung für die Allgemeinheit nicht nur „schmückendes Beiwerk“ des Online-Angebotes sein darf. Erforderlich ist nach dem BGH in dieser Hinsicht ein Mindestmaß an eigener inhaltlicher Bearbeitung der bereitgestellten Informationen[43]. Eine geringe Relevanzschwelle wurde mit dieser Formulierung zumindest eingezogen, um einfachste Banalitäten auszuklammern.

Fazit: Eine Recherche von Privatpersonen mit dem Zweck, die Presse zu informieren, fällt nach den hier erläuterten Argumenten unter den Anwendungsbereich des Medienprivilegs, wenn darunter ein Beitrag zur Meinungsbildung für die Öffentlichkeit zu erkennen ist und die Recherche ausschließlich zu diesem Zweck erfolgt ist.

6.3.4 Anwendung des Medienprivilegs auf Online-Medienarchive

Die Frage, ob sich die Privilegierung des Art. 85 DSGVO auch auf online zur Verfügung gestellte Medienarchive erstreckt, lässt sich leichter beantworten, denn im Erwägungsgrund 153 S. 3 zur DSGVO werden „Nachrichten- und Pressearchive“ ausdrücklich als Anwendungsbereich erwähnt.

[38] Siehe auch: Pötters, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO Art. 85, Rn. 8
[39] Buchner/Tinnefeld, in: Kühling/Buchner, 4. Aufl. 2024, DS-GVO Art. 85, Rn. 14
[40] Cornils, in: BeckOK InfoMedienR, 41. Ed. 1.2.2021, DS-GVO Art. 85, Rn. 70.1-70.2
[41] BGHZ 181, 328, Rn. 21
[42] EuGH, Urt. v. 14.02.2019 – C 345/17, Rn. 57 – Buivids
[43] BGH Urt. v. 12.12.2021 – VI ZR 488/19

Pressearchiv ist dabei als Archiv mit journalistischen Inhalten zu verstehen. Auch Online-Archive, die ein Medienunternehmen zu journalistisch-redaktionellen Zwecken erstellt und die es zeitlich unbefristet außerhalb seines aktuellen Angebots und als Altinhalte gekennzeichnet über seine Telemedien-Angebote im Internet zum Abruf bereithält, unterfallen nach den angestellten Erwägungen zur Auslegung dem Medienprivileg.[44] Die Anwendungsbereiche des Medienprivilegs haben eine hohe Relevanz für die Tätigkeit der Rundfunkanstalten im redaktionellen Bereich, genauso wie in der datenschutzkonformen Erfüllung von Verwaltungsaufgaben. Es werden sich daher sicherlich weitere Grenzbereiche ergeben, zu denen ich in kommenden Tätigkeitsberichten Stellung zu nehmen beabsichtige.

6.4 Programmbeschwerden: namentliche Nennung von Beschwerdeführern?

Die Rundfunk-, Fernseh- und Hörfunkräte der Rundfunkanstalten haben darüber zu wachen, dass der jeweilige staatsvertragliche oder gesetzliche (Programm-)Auftrag erfüllt wird. Im Zuge dieser Aufgabe erfüllen sie die Pflicht, sich mit Programmbeschwerden von Bürgerinnen und Bürgern auseinanderzusetzen. Regelmäßig werden solcherlei Beschwerden in den jeweils zuständigen Ausschüssen der Gremien bearbeitet. Die Tagesordnungen zu diesen Ausschüssen sind teilweise öffentlich und jedermann zugänglich.

Mich erreichte im Berichtsjahr eine Beschwerde, in der moniert wurde, dass auf einer Tagesordnung einer solchen Sitzung der Name des Beschwerdeführers mit samt seiner Programmbeschwerde genannt wurde. Ich hatte zu prüfen, ob dies datenschutzrechtlich in Ordnung ist.

Die verantwortliche Rundfunkanstalt bzw. das Gremium hat sich auf eine interne Regel berufen, nach der die Tagesordnungen der Ausschüsse zu veröffentlichen seien. Es wurde argumentiert, dass jemand, der eine förmliche Programmbeschwerde einlege, auch mit einer gewissen Öffentlichkeit seines Namens zu rechnen habe.

Dies konnte von mir so nicht akzeptiert werden, da es für die Veröffentlichung einer Programmbeschwerde nicht darauf ankommt, wer sie konkret eingelegt hat. Natürlich kann transparent über Programmbeschwerden berichtet werden, jedoch kann die Rechtsgrundlage nicht rechtfertigen oder gar erfordern, dass auch Namen von Beschwerdeführern veröffentlicht werden. Dies ist eine unzulässige Ausweitung der Transparenzvorgaben, die sich eben nicht auf personenbezogenen Daten beziehen, die in keinem Zusammenhang mit dem

[44] Hennemann, in: Specht/Mantz, DatenschutzR-HdB § 19, Rn. 110 ff.

Beschwerdegegenstand stehen: Wofür sollte es wichtig sein zu wissen, wer genau eine Beschwerde zum Programm eingelegt hat?

In Zukunft - und dies habe ich dem Beschwerdeführer mitgeteilt - wird diese Praxis so nicht mehr fortgeführt werden. Insofern hatte die betreffende Rundfunkanstalt hier gegen Datenschutzvorschriften verstoßen, was allerdings auf einem Versehen bzw. einer unrichtigen Interpretation der internen Vorschrift beruhte. Ich habe die entsprechende Rundfunkanstalt aufgefordert, die Mitarbeitenden noch besser für das Thema Datenschutz zu sensibilisieren, damit solcherlei Fehleinschätzungen nicht mehr vorkommen. Der Beschwerde konnte ich insoweit abhelfen.

6.5 ARD-Diversity Umfrage

Ein Thema, das auch den AK DSB beschäftigt hat, war die ARD-Diversity Umfrage. Der Plan lautete, dass diese Umfrage, die auf freiwilliger Basis stattfindet, dazu dienen sollte, den Rundfunkanstalten einen Überblick über Vielfalt und Diversität bei den Mitarbeitenden zu verschaffen. Damit soll ein Beitrag zur Vielfaltskultur geleistet und Diskriminierung entgegengewirkt werden.

Datenschutzrechtlich interessant ist es vor allem deswegen, weil in großen Teilen sehr sensible Daten zu Herkunft und ggf. Migrationsgeschichte, sexueller Orientierung und Religion erfragt werden. Insgesamt schienen die dem AK DSB vorgelegten Fragen so weitreichend und ausufernd, dass allein schon deshalb ein enormes Risiko gesehen wurde. Ein weiteres Problem erwuchs daraus, dass die mit der Datenerhebung verfolgten Zwecke konkret zu benennen sind, damit eine informierte Einwilligung eingeholt werden kann. Fragen zur sexuellen Orientierung oder Sonstigem, was allein die Privatsphäre betrifft, haben den Arbeitgeber nämlich nichts anzugehen.

Ohne hier ins Detail gehen zu können, hat sich der AK DSB dahingehend positioniert, das Vorhaben trotz der geplanten Anonymität der Umfrage als kritisch einzuordnen. Zumindest muss in jenem Fall eingehend geprüft werden, ob eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO durchzuführen ist. Auch müssen dem Schutzbedarf angemessene technische und organisatorische Maßnahmen zur Datensicherheit vorgesehen werden, die angesichts der kritischen und sensiblen Daten ein hohes Sicherheitsniveau gewährleisteten müssten. Schließlich war das Thema der De-Anonymisierung in den Blick zu nehmen: es müsste also in jenem Fall sichergestellt werden, dass die Daten nicht auf eine einzelne Person zurückgeführt werden können. Dies ist ausgehend von den zahlreichen Daten, die abgefragt werden sollen, ein durchaus ernstzunehmendes Risiko. Ebenso muss schon von Anfang an klar sein, wofür die Daten tatsächlich verwendet werden. Mit anderen

Worten: Die Daten dürfen nicht erst erhoben werden und im Anschluss daran wird über davon abgeleitete Maßnahmen befunden.

Nach meinem Wissen ist diese - gewiss sehr gut gemeinte - Umfrage nicht mehr weiterverfolgt worden, was ich begrüße. Aufgrund der hohen Komplexität und des sehr ernstzunehmenden Risikos sind solche Umfragen gemessen an dem daraus geschöpften Wert aus datenschutzrechtlicher Sicht wenig empfehlenswert.

6.6 Baden-Badener Pensionskasse – datenschutzrechtliche Vertragsgestaltung

Die Baden-Badener Pensionskasse (bbp) ist eine Einrichtung der betrieblichen Altersversorgung für die öffentlich-rechtlichen Rundfunkanstalten, deren gewerblicher Töchter und das ZDF, in der Form eines Versicherungsvereins auf Gegenseitigkeit (VVaG). Sie bietet ebenso verschiedene Formen der Direktversicherung an.

Bereits im November 2022 im Rahmen der seinerzeitigen AK DSB-Sitzung hat die damals neue betriebliche Datenschutzbeauftragte der bbp die aus ihrer Sicht nicht mehr aktuellen datenschutzrechtlich relevanten Verträge zwischen den Rundfunkanstalten und der bbp zur Diskussion gestellt.

Insofern musste die Frage geklärt werden, ob die bestehenden Verträge datenschutzrechtlich den Anforderungen entsprechen. Einigkeit bestand darin, dass im Hinblick auf das Kerngeschäft - die Rückdeckung bzw. das Versicherungsgeschäft - die bbp als Verantwortliche im Sinne des Datenschutzes einzuordnen ist und insofern keine Auftragsverarbeitung zu vereinbaren ist. Die bbp verfolgt eigene Ziele und Geschäftszwecke, u.a. im Rahmen der Leistungsfeststellung, der Berechnung des individuellen Versorgungsbeitrags für bestimmte Tarife, für die Berechnung der versicherungstechnischen Werte und der Berechnung der zu versichernden Rentenhöhe und Rentenbausteine sowie die Auszahlung der Versicherungsleistung. Dies ist nicht zu beanstanden und wurde auch nicht problematisiert.

Schwieriger zu beurteilen war hingegen, was in der Leistungsphase und der Abrechnung und Auszahlung von Renten zu gelten hat. Es wurde angeführt, dass im Hinblick auf die Schwerpunkttheorie keine Auftragsverarbeitung vorliegen könne. Der Schwerpunkt der Leistung liege nämlich nicht in der Verarbeitung personenbezogener Daten, sondern vielmehr in der Berechnung und Auszahlung von Renten.

Als Aufsicht bin ich der Auffassung gefolgt, dass die Frage nach der Entscheidung über die wesentlichen Mittel und Zwecke der Datenverarbeitung zu verknüpfen ist mit der Frage, welchen Schwerpunkt die (eigentliche) Dienstleistung hat. Wenn der Datenverarbeitung im Rahmen der Dienstleistung kein allzu hohes und gleichsam überwiegendes Gewicht beizumessen ist, und die Mittel und Zwecke der Datenverarbeitung - zumindest auch - vom Auftragnehmer bestimmt werden, so kann die Schwerpunkttheorie greifen und von einer alleinigen Verantwortung des Auftragnehmers ausgegangen werden. Dies ist beispielsweise dann der Fall, wenn die Datenverarbeitung nur Mittel und Zweck ist, um eine andere Dienstleistung umzusetzen und diese Datenverarbeitung von Umfang und Risiko eher als gering einzuschätzen ist.

Also kann im Umkehrschluss auch eine nicht direkt auf die Datenverarbeitung als Vertragsgegenstand abzielende Dienstleistung dann als Auftragsverarbeitung angesehen werden, wenn die Datenverarbeitung für die geschuldete Dienstleistung eine entscheidende Bedeutung hat.

Es schien mir im vorliegenden Fall unter Berücksichtigung aller Umstände angemessen und richtig, bei der Beauftragung der Auszahlung der Renten in der Leistungsphase eine Auftragsverarbeitung zwischen den Rundfunkanstalten und der Baden-Badener Pensionskasse anzunehmen, weil die Berechnung und Auszahlung der Renten auf vollständig von den Rundfunkanstalten vorgegebenen Datenverarbeitungen beruhen, die ein höheres Gewicht im Vergleich zum eigentlichen Leistungsgegenstand, also der Auszahlung der Renten, haben.

Hieran ist gut zu erkennen, dass jeder Fall anders gelagert sein kann und im Einzelfall intensiv zu prüfen ist, welche Art von Verträgen abzuschließen sind.

6.7 Datenschutz in den Rundfunkanstalten

Bereits an verschiedenen Stellen habe ich in diesem Bericht auf meinen Anspruch hingewiesen, auch einen Überblick über die Datenschutzrealität in den einzelnen von mir beaufsichtigten Rundfunkanstalten geben zu können. Dies ist ein ambitioniertes Ziel, denn die Aufsicht über neun Rundfunkanstalten und die entsprechenden Beteiligungsunternehmen erlauben es nicht, im Detail in den Datenschutz der einzelnen Bereiche hineinzusehen. Dennoch soll in den nächsten Jahren ein Informationssystem über regelmäßige Jour Fixes aufgebaut werden, das mir einen möglichst tiefen Einblick erlauben und mir gleichzeitig den Freiraum erhalten soll, Datenschutzaufsicht in der Form auszuüben, wie sie notwendig ist. Diese beinhaltet in meinen Augen insbesondere übergreifende Audits und Prüfungen von bestimmten datenschutzrechtlichen Themen (Datenschutzmanagementsystem, VVT, Nutzungsmessung, Apps, etc.) und die Beratung auf Anfrage. Da ich auch zuständig bin für Beschwerdebearbeitungen, die mir aufgrund der gesetzlichen

Aufgabenzuweisung obliegt, bin ich an dieser Stelle gehalten, die Ressourcen entsprechend einzusetzen.

Im Berichtsjahr fand der soeben skizzierte regelmäßige detaillierte (Einzel-) Austausch mit den Rundfunkanstalten noch nicht statt. Ich habe daher die jeweiligen Datenschutzbeauftragten gebeten, mir kurz die Schwerpunkte ihrer Arbeit zu skizzieren, damit ich einen ersten Überblick gleichsam als Ausgangspunkt für weitere Einblicke bekomme.

In sämtlichen Rundfunkanstalten steht das Thema Einführung und Erweiterung von M365 Funktionalitäten - auch im Zusammenhang mit Anwendung zur Künstlichen Intelligenz - im Fokus der Tätigkeiten. Ebenso ist der Auf- und/oder Ausbau des Datenschutzmanagementsystems (DSMS) ein Schwerpunkt. Die Ausbaustufen sind noch recht unterschiedlich ausgeprägt: Es hat sich gezeigt, dass verschiedene Rundfunkanstalten schon sehr weit sind mit der Entwicklung und dem Einsatz eines solchen Systems, bei anderen hingegen der Aufbau mit Nachdruck vorangetrieben wird. Hier ist von Bedeutung, dass die Aufsicht die Entwicklungen im Blick behält und die entscheidenden Impulse und Hinweise gibt, falls es „hakt“ oder nicht weitergeht. Der AK DSB hat ein entsprechendes Hinweispapier zum Thema Aufbau eines DSMS erarbeitet, das gewiss hilfreich ist (Kapitel 8.2).

Ein wichtiges Thema für die Datenschutzbeauftragten ist auch stets die Ausprägung ihrer Rolle, also die Beantwortung der Frage, was tatsächlich die Pflichten und Aufgaben einer oder eines Datenschutzbeauftragten sind. Hierbei ist immer zu beachten, dass die Datenschutzbeauftragten unabhängig agieren können, aber dennoch in die Datenschutzprozesse und Fragestellungen der einzelnen Verantwortlichen eng eingebunden sind. Im Einzelfall kann es zu Abgrenzungsschwierigkeiten kommen, auch für solcherlei Fragen steht der Rundfunkdatenschutzbeauftragte als Ansprechpartner gern bereit.

Weitere Themen waren die Einführung von SAP, die Führung von Verzeichnissen von Verarbeitungstätigkeiten und die Beschäftigung mit dem Audit des Rundfunkdatenschutzbeauftragten zur Nutzungsmessung.

Auf eine weitere Einengung auf einzelne Themen soll an dieser Stelle und in diesem Bericht (noch) verzichtet werden, da ein fundierter Einblick aus den oben genannten Gründen fehlt. Ich bin aber - um auch dies zu wiederholen - guten Mutes, dass dies im laufenden Jahr anders wird, insbesondere auch deswegen, weil mir durch eine zusätzliche Mitarbeiterin weitere Kapazitäten zur Verfügung stehen.

6.8 Datenschutz beim Beitragsservice

Der Beitragsservice von ARD, ZDF und Deutschlandradio verwaltet die Daten der Rundfunkbeitragszahlerinnen und -zahler in einem Rechenzentrum zentral in Köln. Klagen sowie Rechtsangelegenheiten werden dagegen dezentral von den einzelnen Rundfunkanstalten betreut.

Die Rundfunkdatenschutzbeauftragten übernehmen die datenschutzrechtliche Kontrolle über die Verarbeitung der Daten beim Beitragsservice. Rechtliche Grundlage sind die Regelungen der einzelnen Landesrundfunkanstalten. Bei Radio Bremen und beim Hessischen Rundfunk besteht eine Ausnahme. Die dortigen Landesdatenschutzbeauftragten üben die Kontrollfunktion aufgrund der sogenannten geteilten Zuständigkeit aus. Oft ist angeklungen, dass unter dem Gesichtspunkt der Staatsferne des Rundfunks diese Konstruktion verfassungsrechtlichen Bedenken begegnet. Dies galt im Berichtsjahr auch noch für den rbb, was sich jedoch seit dem 01.01.2024 geändert hat und es eine insoweit ungeteilte Zuständigkeit des Rundfunkdatenschutzbeauftragten gibt (siehe hierzu auch Kapitel 1.1).

Der interne Datenschutz beim zentralen Beitragsservice obliegt einer behördlichen Datenschutzbeauftragten nach § 11 Abs. 2 Rundfunkbeitragsstaatsvertrag. Mit ihr und ihrem Stellvertreter besteht ein enger Kontakt, insbesondere im Zusammenhang mit Stellungnahmen zu den zahlreichen Beschwerden. Die sehr freundliche und professionelle Zusammenarbeit soll an dieser Stelle ausdrücklich gewürdigt werden, Frau Katharina Aye und Herrn Christian Kruse gebührt mein Dank und Respekt.

Stets berichtet die behördliche Datenschutzbeauftragte überdies im AK DSB, beteiligt sich an den dortigen Diskussionen und wirkt an der Lösung von Rechtsfragen mit. Ab dem Jahr 2024 hat Frau Aye überdies den Vorsitz des AK DSB übernommen.

Aufsichtsrechtlich steht die RDSK mit dem Beitragsservice in stetigem Austausch, es wird regelmäßig über verschiedene Themen gesprochen. Dies betrifft Auslegungsfragen zu Urteilen ebenso wie Einzelfragen zu bestimmten Verarbeitungen. Die nachstehenden Beispiele sollen dies verdeutlichen.

6.8.1 Auskunftsersuchen und Betroffenenrechte

Der Beitragsservice stellt insbesondere für Auskunftsersuchen nach § 11 Abs. 8 des Rundfunkbeitragsstaatsvertrages (RBStV) ein entsprechendes Formular zur Verfügung, das gemäß § 12 Abs. 2 DSGVO der Erleichterung der Ausübung von Betroffenenrechten dienen soll. Es kommt aber auch vor, dass Auskunftsersuchen über die E-Mail-Adresse impressum@rundfunkbeitrag.de

gestellt werden. Im Zuge dessen wurde gemeinsam mit der Datenschutzbeauftragten des Beitragsservice und ihrem Stellvertreter die Frage diskutiert, ob bei dieser Adresse eingehende Auskunftsersuchen bearbeitet werden müssen oder ob dies ggf. nicht verpflichtend ist.

Der Rundfunkdatenschutzbeauftragte vertritt die Auffassung, dass als Mindeststandard beim Umgang mit Auskunftsersuchen über eine eigentlich nicht dafür vorgesehene E-Mail-Adresse des Verantwortlichen eine Antwort mit Hinweis auf einen entsprechenden anderen Weg oder ein taugliches Formular ergehen muss, oder alternativ der Antrag direkt in die richtige Stelle beim Verantwortlichen zur Bearbeitung weitergeleitet wird. Die E-Mails dürfen nicht ins Leere laufen und machen eine Antwort in aller Regel erforderlich, auch wenn die aus Artikel 12 Abs. 3 Satz 1 DSGVO gegebene Frist zur Beantwortung eines Auskunftsersuchens möglicherweise noch nicht zu laufen beginnt.

Im Zuge dessen wurde auch die Frage diskutiert, wie man flankierend den Zugang zu den richtigen Auskunftswegen verbessern kann, damit die einzig öffentlich verfügbare E-Mail-Adresse impressum@rundfunkbeitrag.de nicht für diese eigentlich sachfremden Zwecke verwendet wird. Ich habe deshalb darauf gedrungen, die datenschutz-spezifischen Formulare sichtbarer und leichter auffindbar auf der Internetseite www.rundfunkbeitrag.de zu platzieren. Bisher waren diese nur in der Rubrik „Datenschutz“ erreichbar, nicht jedoch über den sehr ausführlich gestalteten Kontaktbereich der Website des Beitragsservice. Sowohl die Formulare zu Datenschutz-Themen, als auch das Datenschutzkontaktformular und die Anfrage zur Auskunft über gespeicherte Daten sollten auch über diese Rubrik auffindbar sein, entweder über eine Platzierung bei den thematisch sortierten Kontaktanliegen oder zumindest über einen Link zu den Datenschutzformularen.

Der Beitragsservice hat umgehend reagiert und bereits Anfang Dezember des Berichtsjahres vermeldet, dass die Onlineformulare zur Beantragung einer Datenauskunft prägnanter platziert worden sind. Eine Überprüfung hat ergeben, dass auf der Seite www.rundfunkbeitrag.de lediglich zwei Klicks notwendig sind, um das entsprechende Auskunftsformular zu erreichen. Diese Navigation ist auch weit oben auf der Startseite des Angebots platziert.

Damit ist zumindest erreicht, dass eine Auskunft leichter beantragt werden kann und - so steht zu hoffen - die Adresse impressum@rundfunkbeitrag.de nicht mehr so häufig verwendet wird. (Es war im Übrigen vorgekommen, dass Auskunftsersuchen über diese Adresse nicht in der erforderlichen Weise bearbeitet worden waren.)

Ob diese Korrektur zu den gewünschten Ergebnissen geführt hat, kann erst im kommenden Jahr überprüft werden. Es ist aber davon auszugehen, dass die entsprechenden Effekte erzielt werden.

6.8.2 Auskunft zu konkreten Empfängern

Der EuGH hat in seiner Entscheidung vom 12.01.2023 (C-154/21) entschieden, Art. 15 Abs. 1 lit. c) DSGVO dahingehend auszulegen, dass das in dieser Bestimmung vorgesehene Recht der betroffenen Person auf Auskunft über die sie betreffende personenbezogenen Daten bedingt, dass der Verantwortliche, wenn diese Daten gegenüber Empfängern offengelegt worden sind oder noch offengelegt werden, verpflichtet ist, der betroffenen Person die Identität der Empfänger mitzuteilen. Mit dieser Entscheidung hat der EuGH die Betroffenenrechte gestärkt und klargestellt, dass die Betroffenen wählen können, ob ihnen die konkreten Empfänger oder lediglich Empfängerkategorien mitgeteilt werden.

Im Rahmen des Beitragseinzugs gibt es die Spezialvorschrift des § 11 Abs. 8 Rundfunkbeitragsstaatsvertrag (RBStV), die vorsieht, lediglich über die in § 8 Abs. 4 RBStV genannten personenbezogenen Daten, das Bestehen, den Grund, die Dauer einer Befreiung oder Ermäßigung im Sinne der §§ 4 und 4a RBStV, die betreffenden Bankverbindungsdaten und die Stelle, die die jeweiligen Daten übermittelt hat, zu informieren. Es war die Frage zu bewerten, ob es sich hiermit um eine Vorschrift mit abschließender Wirkung handelt oder ob diese Vorgabe im Licht des Urteils des EuGH neu zu bewerten ist.

Die RDSK hat dieses Thema beraten und ist zu folgendem Schluss gekommen:

§ 11 Abs. 8 RBStV ist die für den Beitragseinzug und damit für die Landesrundfunkanstalten einschlägige Vorschrift. Auskünfte, die nach dieser Maßgabe erteilt werden, sind insoweit als vollständig anzusehen. Die öffentliche Verwaltung, zu der die Rundfunkanstalten bzw. der in ihrem Auftrag handelnde Beitragsservice zu zählen sind, soweit es um die Feststellung der Pflicht zur Zahlung des Rundfunkbeitrags sowie die Abwicklung des damit verbundenen Verwaltungsverfahrens geht, hat die für sie maßgeblichen formellen und materiellen Gesetze anzuwenden, solange und soweit sie nicht für ungültig bzw. unwirksam erklärt worden sind. Eine solche Feststellung ist mit Bezug auf Gesetze im formellen Sinne den Verwaltungsgerichten, in Bezug auf Gesetze im materiellen Sinne hingegen ausschließlich dem Bundesverfassungsgericht oder dem Europäischen Gerichtshof vorbehalten. Ausgehend von dieser Argumentation kann ausschließlich der EuGH verbindlich feststellen, ob diese Vorschrift mit Art. 15 DSGVO unvereinbar ist.

Die hier gegenständliche Entscheidung des EuGH zur Auslegung des Art. 15 Abs. 1 lit. c) DSGVO ist dafür nach Auffassung der RDSK jedoch nicht geeignet. Wäre dies der Fall, müsste Art. 15 DSGVO ohnehin auf den Beitragseinzug und die damit zusammenhängenden Auskunftsersuchen angewendet werden und nicht § 11 Abs. 8 RBStV. Im Ergebnis besteht aus der Sicht der RDSK keine

Pflicht des Beitragsservice von ARD, ZDF und Deutschlandradio die bisherige Praxis zu ändern und über konkrete Empfänger im Rahmen des Beitragseinzugs zu unterrichten.

6.8.3 Reichweitenanalyse und Cookie-Banner

Im Berichtsjahr erreichten mich verschiedene Beschwerden zum Cookie-Banner oder auch Einwilligungs-Banner des Beitragsservice von ARD, ZDF und Deutschlandradio (siehe auch Kapitel 3.4.3).

Der Beitragsservice ist zu Recht daran interessiert, wie seine Serviceangebote auf der Website rundfunkbeitrag.de angenommen werden, und ob sie ggf. verändert oder verbessert werden sollten. Dies entspringt sowohl dem Servicegedanken, dass man es den Rundfunkbeitragszahlern so einfach wie möglich machen sollte, bestimmte Informationen an den Beitragsservice weiterzuleiten, parallel wird der Zweck verfolgt, die Seiten benutzerfreundlicher zu gestalten.

Die Rundfunkdatenschutzbeauftragten vertreten die Auffassung, dass eine anonymisierte Nutzungsmessung der **publizistischen Angebote** der Rundfunkanstalten bei kurzzeitiger Verarbeitung und der sofortigen Kürzung der IP-Adresse gemäß Art. 6 Abs. 1 lit. e) DSGVO i.V.m. § 30 Abs. 3 Medienstaatsvertrag zulässig ist, wenn damit eine Anonymisierung erreicht wird.[45] Hintergrund dieser Rechtsauffassung ist, dass die Rundfunkanstalten mit ihren journalistischen Angeboten gehalten sind, diese zeitgemäß zu gestalten, um allen Bevölkerungsgruppen die Teilhabe an der Informationsgesellschaft zu ermöglichen und damit dem verfassungsrechtlichen Auftrag zu erfüllen. Bei solcherlei Angeboten ist die Nutzungsmessung ohne Einwilligung der Nutzer zulässig, ebenso auch unter Berücksichtigung des § 25 Abs. 2 Nr. 2 TTDSG. Die publizistischen Angebote der öffentlich-rechtlichen Rundfunkanstalten müssen im Wettbewerb bestmöglich konkurrieren können, dafür sind alle Erkenntnismöglichkeiten zur Wirkung, Reichweite und Akzeptanz der Angebote und Inhalte auszuschöpfen und das Angebot stetig weiter zu entwickeln. Nach Auffassung der Rundfunkdatenschutzbeauftragten ist eine zu diesem Zweck durchgeführte anonymisierte Nutzungsmessung für die Rundfunkanstalten unbedingt erforderlich, um einen vom Nutzer bzw. letztendlich von der Gesamtheit aller Nutzenden ausdrücklich gewünschten Telemediendienste zur Verfügung zu stellen (siehe hierzu ausführlich Kapitel 6.1.1).

Nach meiner Auffassung unterscheidet sich diese Nutzungsmessung der Rundfunkanstalten von derjenigen bei www.rundfunkbeitrag.de.

[45] Hinzuweisen ist an dieser Stelle auf die aktuelle Rechtsprechung zur Anonymisierung, die von der Notwendigkeit einer absoluten Anonymisierung zugunsten einer relativen Anonymisierung abrückt (siehe dazu Kapitel 3.4.1).

Im Gegensatz zu den redaktionell gestalten Angeboten der Rundfundanstalten steht die Website des Rundfunkbeitrags nicht im publizistischen Wettbewerb. Sie dient - wie oben schon aufgeführt - eher der Verbesserung des Beitragseinzugs und unterstützt damit die entsprechende staatsvertragliche Pflicht. Eine explizite Pflicht, ein Online-Angebot bereit zu stellen, findet sich indes nicht im Rundfunkbeitragsstaatsvertrag. Der in der Vorschrift des TTDSG vorausgesetzte ausdrückliche Wunsch der Nutzenden (wenngleich objektiviert) und ebenso die damit verknüpfte Erforderlichkeit können sich nicht auf die mit der Aufgabe generell begründete Notwendigkeit beziehen, eine effektive zeitgemäße Website bereit zu stellen. Ein objektiv und gut begründeter Nutzen allein kann nicht genügen, denn das TTDSG dient der Abwehr von Eingriffen in die Privatsphäre und stellt die subjektive Perspektive in den Vordergrund.

Das bedeutet im konkreten Fall, dass der Beitragsservice auch unabhängig von einwilligungsfreier Nutzungsmessung seine Online-Angebote bereitstellen könnte. Eine unbedingte Erforderlichkeit der Nutzungsmessung ohne Einwilligung unter Berücksichtigung des Nutzerwunsches kann nicht erkannt werden. Damit besteht ein sehr deutlicher Unterschied zwischen der Bereitstellung von den redaktionellen Angeboten der Rundfunkanstalten und der gleichsam begleitenden und unterstützenden Onlinepräsenz des Beitragsservice.

Diskutiert wurde auch in diesem Zusammenhang, dass die französische Datenschutz-Aufsichtsbehörde CNIL für Frankreich offensichtlich eine generelle Ausnahme hinsichtlich der anonymisierten Nutzungsmessung für denkbar hält (siehe auch Kapitel 6.1.1).[46] In diesem Zusammenhang wurde auch darüber nachgedacht, dass allein aus datenschutzrechtlicher Perspektive eine Einwilligung vielleicht nicht notwendig ist, weil die Nutzungsmessung zur Herstellung eines leistungsfähigen und dem Beitragseinzug dienenden Angebotes dem Auftrag des Beitragsservice aus dem Rundfunkbeitragsstaatsvertrag entspricht. Allerdings habe ich mir hierzu keine abschließende Meinung gebildet, da die vorstehenden Erwägungen zum TTDSG einer einwilligungsfreien Nutzungsmessung aus meiner Sicht zurzeit noch entgegenstehen.

Verschiedene Beschwerden hatten darauf hingewiesen, dass das bisherige Cookie-Banner des Beitragsservice von ARD, ZDF und Deutschlandradio die Ablehn-Möglichkeit der Nutzungsmessung auf erster Ebene nicht in der erforderlichen transparenten Form ermöglicht. Daher wurde der Beitragsservice aufgefordert (und es konnte insofern auch Einigung erzielt werden), dass das Cookie-Einwilligungsbanner beim erstmaligen Aufruf der Seite www.rundfunkbeitrag.de in der Form umgestaltet wird, dass die Ablehn-Möglichkeit in gleicher Größe, Form und Farbe neben der Zustimmung zur anonymisierten Nutzungsmessung erscheint. Insofern wurde auch die aktuelle Rechtsprechung (siehe auch Kapitel 3.4.3) berücksichtigt, die eine entsprechende freiwillige

[46] https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-daudience

Einwilligung von einer solchen Gestaltung abhängig macht. Hintergrund dieser Rechtsprechung ist, dass den Nutzerinnen und Nutzern eine gleichwertige Auswahlmöglichkeit zur Verfügung gestellt wird, damit gleichsam eine freiwillige Entscheidung gefällt werden kann, ohne in eine bestimmte Richtung gedrängt oder gelenkt zu werden.

Ich bin der Auffassung, dass hiermit eine rechtssichere und zufriedenstellende Lösung gefunden wurde. In Zukunft wird sich erweisen, ob eine anonymisierte Nutzungsmessung, die keine Profilbildung zum Ziel hat und lediglich zur Optimierung von Websites gedacht ist, auch ohne Einwilligung möglich ist – wenngleich auch unter strengen und genau zu beachtenden Maßgaben. Hier muss sich letztendlich der Gesetzgeber entscheiden und entsprechende Vorschriften vorlegen.

6.8.4 Meldedatenübermittlung – Zuständigkeit des Rundfunkdatenschutzbeauftragten?

Es kommt vor, dass ich mit Beschwerden konfrontiert bin, bei denen ich mich auch mit meiner Zuständigkeit auseinanderzusetzen habe. Grundsätzlich ist diese immer dann berührt, wenn die angegriffene Datenverarbeitung in Verantwortung der mir zugeordneten Rundfunkanstalten stattfindet.

In diesem Fall ging es um die Datenübermittlung einer Gemeinde in Baden-Württemberg an den Beitragsservice. Ein Betroffener, der jüngst in die Stadt gezogen war, hatte sich an die Gemeinde gewandt und um die Unterbindung der Weiterleitung seiner Daten an den Beitragsservice oder den SWR nachgesucht. Die Stadt war grundsätzlich der Auffassung, dass ein Widerspruch gegen eine solche Verpflichtung nicht möglich sei, hat diese Beschwerde aber dennoch an mich weitergeleitet.

Zunächst hatte ich mir die Frage zu stellen, wer für die gegenständliche Datenverarbeitung verantwortlich ist. § 13 der Verordnung des Innenministeriums für Durchführung des baden-württembergischen Ausführungsgesetzes zum Bundesmeldegesetz (Meldeverordnung-MVO) lieferte Aufschluss: In der Vorschrift ist die Datenübermittlung an den Südwestrundfunk geregelt. Dort ist festgelegt, dass die jeweilige Meldebehörde dem SWR oder dem Beitragsservice zum Zwecke der Erhebung und Einzug der Rundfunkbeiträge im Falle der Anmeldung, Abmeldung oder des Todes bestimmte Daten volljähriger Personen aus dem Melderegister übermittelt. In der Tat ist die Übermittlung dieser Daten durch die Meldebehörde an den SWR also gesetzlich geregelt und insofern rechtlich bindend im Sinne von Art. 6 Abs. 1 lit. c) DSGVO. Diese Vorschrift adressiert untermittelbar die jeweilige Meldebehörde, die dann auch als Verantwortliche im Sinne des Datenschutzes anzusehen ist. Meine Aufsichtszuständigkeit war insofern nicht berührt, obwohl es sich um Daten handelte, die dem Beitragseinzug dienen, weshalb der Irrtum dieser Gemeinde durchaus nachvollziehbar ist. Richtigerweise hat die Gemeinde aber eingeschätzt, dass gegen eine solch pflichtige Datenverarbeitung keine Widerspruchsmöglichkeit besteht. Natürlich kann

unabhängig davon eine Beschwerde eingelegt werden, in Ansehung des Verantwortlichen aber nicht bei mir, sondern beim zuständigen Landesdatenschutzbeauftragten – hier des Landes Baden-Württemberg.

6.9 Datenschutz beim KiKA

Der Kinderkanal KiKA ist eine Gemeinschaftseinrichtung von ARD und ZDF, deren Federführung beim Mitteldeutschen Rundfunk liegt. Datenschutzrechtlich können hier deswegen besondere Probleme entstehen, weil unter Umständen Kinderdaten verarbeitet werden. Dies ist eher selten und nur in sehr begrenztem Umfang der Fall, aber im Rahmen von Mitmachaktionen oder auch bei Nutzung der Player-App ist dies zumindest nicht auszuschließen. In meinem vorherigen Bericht zum Jahr 2022 habe ich unter Ziffer 6.1 zu Mitmachaktionen im Rahmen des Programmangebotes Erörterungen angestellt.

Im Berichtsjahr konnte der Fokus nicht in der bisherigen Weise auf den Kinderkanal gerichtet werden, dennoch bestand ein enger Austausch mit dem betrieblichen Datenschutzbeauftragten des KiKA, Herrn Jörn Voss, dem ich für seine Zusammenarbeit und langjährige professionelle Handhabung des Datenschutzes beim Kinderkanal recht herzlich danke.

Anfang des Jahres hatte ich mich mit einer Beschwerde zu einer App des Kinderkanals zu befassen. In Rede stand - aufgrund einer Beschwerde - die Nutzung des sogenannten Microsoft Appcenters in der KiKA-Player App, an das sogenannte Absturzberichte gesendet werden. Informationen über Gerät und Betriebssystem gelangen so an Microsoft. Dies sind die Voraussetzungen, um ein sogenanntes Crashreporting überhaupt anbieten zu können. Damit soll ermöglicht werden, technische Fehler zu analysieren und die Stabilität des Angebots zu gewährleisten. Cookies zur Fehleranalyse und zu Sicherheitszwecken werden auch in der Kommentierung als unbedingt erforderlich im Sinne des TTDSG angesehen[47], was zur Entbehrlichkeit einer Einwilligung führt oder zumindest führen kann. Die Argumentation folgt diesen Überlegungen:

Der KiKA hat ein stabiles Angebot bereitzustellen, das sowohl den technischen als auch den inhaltlichen Anforderungen vollumfänglich entspricht. Dazu gehört auch gerade am Anfang der Veröffentlichung einer solchen App, dass unverzüglich und zielgenau ermittelt und geklärt werden kann, wo die technischen Fehler und Schwierigkeiten liegen, sodass schnell Abhilfe geschaffen werden kann. Gerade bei Angeboten für Kinder muss erwartet werden, dass das Angebot stabil funktioniert, damit die ohnehin noch nicht ausgeprägte Aufmerksamkeitsspanne der jungen

[47] Schneider, in: Assion, Handkommentar TTDSG, § 25 Rn. 37 m.w.N.

Nutzerinnen und Nutzer nicht über Gebühr belastet wird. Die Absturzberichte dienen dem Zweck, die App zu verbessern, technisch stabiler zu gestalten und insgesamt zu perfektionieren. Dies dient zuallererst - und dies folgt auch aus dem Auftrag des öffentlich-rechtlichen Rundfunks - den Interessen der Nutzenden der App.

Man muss aber ebenso sehen: Diese Art Cookies sind aus technischer Sicht insofern nicht „unbedingt erforderlich“, als dass der gesamte Dienst ohne Cookies in keiner Weise mehr nutzbar wäre. Jedoch halte ich es für vertretbar, Cookies für Fehleranalysen und zu Sicherheitszwecken vom Einwilligungserfordernis auszunehmen, wenn die sonstigen datenschutzrechtlichen Voraussetzungen beachtet werden.

Dies gilt jedoch nur dann, wenn Klarheit und Transparenz herrscht und die Verwender solcher Cookies genau wissen, wie die Datenverarbeitung abläuft. Ein Austausch mit der Rundfunkanstalt (hier dem MDR) und den Vertretern des Programmes (KiKA) hat ergeben, dass die Sachlage hinsichtlich der Absturzberichte und auch der Daten, die an das Appcenter gesendet werden, nicht vollständig klar war. Es konnte nicht substantiiert nachgehalten werden, dass die Daten tatsächlich - wie ursprünglich vom Verantwortlichen angenommen - in Europa verbleiben und nicht in die USA übermittelt werden. Daher habe ich veranlasst, dass das Microsoft Appcenter aus der KiKA-Player App zu entfernen ist.

Hieran ist zu erkennen, dass es teilweise äußerst komplex und für die Rundfunkanstalten schwer nachzuhalten ist, welche technischen Eigenschaften einer bestimmten App-Programmierung zu welchen Datenverarbeitungen führen können. Dies ist aber unerlässlich zu wissen, damit eine vollständige Transparenz gegenüber den Nutzenden solcher Angebote sichergestellt werden kann. Diese Beschwerde bzw. dieser Sachverhalt hat mich veranlasst, die Prüfung der Apps der mir zugeordneten Rundfunkanstalten (hier ist eine geeignete Auswahl zu treffen) in meinen Prüf- und Auditplan als Datenschutzaufsicht aufzunehmen. Dies ist entweder noch im Jahr 2024 anzugehen, spätestens jedoch im Jahr 2025.

7 Rundfunkdatenschutzkonferenz (RDSK)

Die Rundfunkdatenschutzbeauftragten haben sich in der Rundfunkdatenschutzkonferenz (RDSK) zusammengeschlossen. Im Berichtsjahr bestand die RDSK aus fünf Personen (ab 01.07.2023 mit Ausscheiden von Frau Anke Naujock-Simon (rbb) 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 11.6 entnommen werden. Im Berichtsjahr haben Sitzungen der RDSK am

26.04.2023 und am 27.09.2023 stattgefunden. Den Vorsitz habe ich im Berichtsjahr übernommen und die Stellvertretung hatte Herr Dr. Heiko Neuhoff, der Rundfunkdatenschutzbeauftragte beim Norddeutschen Rundfunk, inne.

7.1 Aufgaben der RDSK

Die Aufgaben der RDSK ergeben sich aus 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 gab es im Berichtsjahr zwei Verwaltungsvereinbarungen, einmal zur Wahrnehmung der Datenschutzaufsicht über die Gemeinschaftsunternehmen der Rundfunkanstalten und zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen. Hier wurden die Zuständigkeiten der RDSK und die einzelnen Federführungen festgelegt. Im Laufe des Berichtsjahres wurde deutlich, dass diese Verwaltungsverarbeitungen überarbeitet werden mussten, was in enger Zusammenarbeit und unter meiner Federführung stattgefunden hat. Es hat sich gezeigt, dass es sinnvoll ist, die Vereinbarungen zu einer zusammenzufassen, die Anfang des Jahres 2024 in Kraft getreten ist[48].

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

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

- Anpassung der Verwaltungsvereinbarungen zur Wahrung der Datenschutzaufsicht über Gemeinschaftseinrichtungen und Gemeinschaftsunternehmen an die geänderte Aufsicht
- Zusammenarbeit mit der DSK, Berichte aus dem AK Medien, dem AK Grundsatz und vom regelmäßigen Austausch mit den staatlichen Aufsichten
- Umgang der RDSK mit dem Leitfaden für datenschutzrechtliche Gestaltung von Websites und Apps für Kinder
- Austausch zu Einwilligungs- und Cookie-Bannern
- Nutzungsmessung und TTDSG
- Orientierungshilfe zum datenschutzkonformen Einsatz von KI im öffentlich-rechtlichen Rundfunk
- Empfehlung der RDSK zum Data Privacy Framework
- Handreichung der RDSK zu Mastodon

[48] siehe unter 11.7 im Anhang

- Reichweite des Medienprivilegs
- Liste der Verarbeitungsvorgänge nach Art. 35 Abs. 4 und 5 DSGVO

Auch wenn die RDSK personell geschrumpft ist, 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 essentiell und von eigenständiger Bedeutung. Im Berichtsjahr hat sich gezeigt, dass die RDSK - vielleicht auch wegen der geringeren Mitgliederzahl - schnell auf aktuelle Entwicklungen und datenschutzrechtliche Themen reagieren kann. Gerade die rasche Erstellung der Orientierungshilfe zum datenschutzkonformen Einsatz von KI erwiesen, dass die Zusammenarbeit in der RDSK gut funktioniert und für die Praxis in den Rundfunkanstalten wichtig ist. Insofern hat sich die im letzten Tätigkeitsbericht geäußerte Befürchtung, dass die RDSK nicht mehr in der gebotenen Form wahrgenommen wird, als unbegründet erwiesen. Ich hoffe, dass wir gemeinsam auf diesem Weg voranschreiten können.

7.2 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.

7.2.1 Handreichung zu Mastodon

Die RDSK hat auf meine Initiative hin eine Handreichung[49] zum sozialen Mikroblogging-Netzwerk Mastodon veröffentlicht. Darin werden Hinweise zur Funktionsweise und der Art und Weise der Datenverarbeitung in diesem Netzwerk gegeben, die ich kurz aufgreifen möchte.

Mastodon, das als nichtkommerzielles Open Source Projekt betrieben wird, gilt als datensichere Alternative zu X (früher Twitter). Ähnlich wie X zeichnet es sich durch das Verbreiten von kurzen Nachrichten aus, auch Bilder, Videos oder Links können geteilt werden.

Mastodon wird nicht allein von einem zentralen Server gehostet, sondern durch die Open-Source-Bereitstellung der Software ist prinzipiell jeder in der Lage, einen eigenen Mastodon-Server, eine

[49] https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/orientierungshilfen/handreichung-der-rdsk-zu-mastodon

sog. „Instanz“ zu betreiben. Sämtliche Server zusammen bilden das dezentrale Microblogging-Netzwerk Mastodon, das zum sogenannten Fediverse (= Federated Universe) gehört.

Hinsichtlich der Nutzerdaten wirkt sich das föderierte System dahingehend aus, dass diese Daten nicht auf zentralen Servern gespeichert werden, sondern dezentral auf tausenden Servern verteilt sind. Im Feed des eigenen Accounts werden die Postings der gefolgten Accounts in chronologischer Weise angezeigt. Es wird kein Algorithmus eingesetzt (so aber bei X [Twitter] oder Facebook), der nach Analyse des Nutzungsverhaltens die Nachrichten auswählt und sortiert, die man zu sehen bekommt. Damit ist die Herkunft der Inhalte transparent.

Das Fediverse und seine Dienste sind tracker- und werbefrei. Aufzeichnungen von Daten, die dazu benutzt werden können, den Nutzenden zu beeinflussen, findet nicht statt. Anders als etwa bei X und Facebook gibt es bei Mastodon keine Aufforderung, das persönliche Adressbuch zur Verfügung zu stellen, um seine Kontakte automatisch auf der neuen Plattform zu finden. Man muss stattdessen selbstständig nach Kontakten suchen.

Der Ort der Datenverarbeitung richtet sich nach der Auswahl der Instanz (= des Servers) auf dem der eigene Account angemeldet wird. Die Instanz kann frei (unter Beachtung der Voraussetzungen der Instanz) gewählt werden. Der Instanzbetreiber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO samt Informations- und Auskunfts-Verpflichtungen aus Art. 13, 14 DSGVO. Es besteht keine gemeinsame Verantwortlichkeit zwischen Instanzbetreibern und Accountinhabern (wie z.B. bei Facebook).

Ich habe als Rundfunkdatenschutzbeauftragter den Mastodon-Account meines Vorgängers Dr. Reinhard Binder (mastodon.social/@RDSB) übernommen. Ausführungen hierzu finden sich auf S. 11 im Abschlussbericht 2022 meines Vorgängers.

Auch die Rundfunkanstalten sind mit mehreren Accounts und auch eigenen Instanzen (z.B. ard.social, zdf.social) auf Mastodon. Die Nutzung von Mastodon durch die Rundfunkanstalten des öffentlich-rechtlichen Rundfunks kann aus datenschutzrechtlicher Perspektive, wie in der Handreichung erläutert, empfohlen werden.

7.2.2 Empfehlungen zum Umgang mit dem Data Privacy Framework (DPF)

Die EU Kommission hat am 10. Juli 2023 den Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der Europäischen Union und den USA angenommen. In diesem Trans-Atlantic Data Privacy Framework (DPF) genannten Beschluss wird bestätigt, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die im Rahmen dieses

Beschlusses aus der EU an US-Unternehmen übermittelt werden. Im Ergebnis postuliert das DPF, dass in den USA ein mit der Europäischen Union vergleichbares Datenschutzniveau besteht.

Bis zur Verabschiedung dieses Entschlusses mussten verschiedene juristische Hürden überwunden werden. Das sogenannte Safe Harbour-Abkommen und das Privacy Shield-Abkommen, die ebenfalls die Datenübermittlung in die USA geregelt hatten, wurden vom EuGH 2015 (EuGH, 06.10.2015 - C-362/14) und 2020 (EuGH, 16.07.2020 - C-311/18) für unwirksam erklärt. Hintergrund war insbesondere, das fehlende Datenschutzniveau und die in den USA mögliche anlasslose Überwachung von EU-Bürgern. Diese Massenüberwachung sei nicht verhältnismäßig im Sinne von Art. 52 der EU-Grundrechtecharta.

Bereits bei Veröffentlichung des aktuellen Beschlusses gab es von verschiedenen Seiten Kritik, sodass zu erwarten ist, dass auch dieses Papier angegriffen und nur für eine gewisse Zeit Bestand haben wird. Zusammenfassend kann man davon ausgehen, dass die Änderungen innerhalb des DPF im Vergleich zum vorangegangenen Privacy Shield-Abkommen nicht als dazu geeignet anzusehen sind, die vom EuGH festgestellten Mängel hinreichend zu beheben.

Dessen ungeachtet besteht aber mit diesem neuen Angemessenheitsbeschluss eine taugliche Rechtsgrundlage für die Übermittlung der Daten in die USA. Dies ist aber nicht die einzige Voraussetzung. Es muss natürlich auch ein gesetzlicher Erlaubnistatbestand vorliegen und weitere Vorgaben der DSGVO, wie ggf. der Abschluss einer Auftragsverarbeitungsvereinbarung, vorliegen.

Die RDSK hat unmittelbar auf die Veröffentlichung dieses Angemessenheitsbeschlusses reagiert: Nachdem Anfang Juli 2023 das Papier veröffentlicht wurde, hat die RDSK bereits Ende Juli eine Empfehlung zum Umgang mit dem Angemessenheitsbeschluss vorgelegt und in den Rundfunkanstalten verteilt. In diesem Papier werden kurz die wesentlichen Rahmenbedingungen und die Historie der Datenübermittlung in die USA umrissen und konkrete Empfehlungen gegeben. Da das DPF seine Wirkung nur dann entfaltet, wenn das Unternehmen, das personenbezogene Daten erhält, entsprechend zertifiziert ist, muss darauf geachtet werden, ob eine entsprechende Zertifizierung vorliegt. Da - wie eben skizziert - die Gefahr besteht, dass der EuGH diesen Angemessenheitsbeschluss für ungültig erklärt, sollten weitere technische Maßnahmen wie bspw. Verschlüsselung eingesetzt werden.

Ebenso empfiehlt die RDSK:

- Das DPF ersetzt nicht den Abschluss von Auftragsverarbeitungsvereinbarungen oder Joint-Controller-Verträgen. Auf den Abschluss entsprechender Vereinbarungen ist weiterhin zu achten.

- Gemäß Art. 13 Abs. 1 lit. f) DSGVO ist der Hinweis auf einen Angemessenheitsbeschluss im Falle eines Drittlandtransfers verpflichtend. Die Datenschutzerklärungen sind entsprechend anzupassen. Bei der Angabe der Datenimporteure muss informiert werden, ob diese aufgrund einer entsprechenden Zertifizierung unter das DPF fallen.
- Die Verarbeitungsverzeichnisse nach Art. 30 DSGVO müssen aktualisiert werden und die Rechtsgrundlage dokumentieren.
- Standardvertragsklauseln behalten ihre Wirksamkeit. Sofern Zusatzgarantien an die Sicherheit der Datenübermittlung in die USA geregelt wurden, ist die Beibehaltung zu empfehlen, falls das DPF unwirksam werden sollte. Die Durchführung von Datentransfer-Folgenabschätzungen (TIAs) ist weiterhin zu empfehlen.
- Das entsprechende RDSK-Papier wurde auf der RDSK Website[50] veröffentlicht.

Nach meinem Dafürhalten hat die RDSK schnell reagiert und damit ein taugliches Mittel geschaffen, damit die Umsetzung des DPF in den Häusern gut funktionieren kann.

7.2.3 Orientierungshilfe KI

Wie unter Kapitel 6.2 bereits erläutert, hat die RDSK im August 2023 eine Orientierungshilfe erarbeitet, die erste Eckpunkte und datenschutzrechtliche Anknüpfungspunkte hinsichtlich des Einsatzes von Künstlicher Intelligenz (insbesondere zunächst zur Erprobung) bieten soll. Dieses Papier ist momentan als interne Orientierungshilfe konzipiert, da sie aufgrund der rasanten Fortentwicklung im Thema KI lediglich einen vorläufigen Charakter aufweist. Die RDSK hat daher gemeinsam entschieden, diese Orientierungshilfe zunächst nicht zu veröffentlichen, ich verweise an dieser Stelle auf die in Kapitel 6.2 beschriebenen wesentlichen Inhalte und Schwerpunkte dieses Papiers.

8 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 hatte im Berichtsjahr die Datenschutzbeauftragten des ZDF und des BR inne. Nach

[50] https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/orientierungshilfen/empfehlung-der-rdsk-zum-umgang-mit-dem-angemessenheitsbeschluss-fuer-den-datenschutzrahmen-zwischen-der-europaeischen-union-und-den-usa

Ausscheiden des Datenschutzbeauftragten des BR hat später im Jahr die Datenschutzbeauftragte des WDR den stellvertretenden Vorsitz übernommen.

8.1 Austausch im AK DSB

Als Rundfunkdatenschutzbeauftragter bei insgesamt neun Rundfunkanstalten nehme ich als Gast an den Sitzungen teil. Es hat sich gezeigt, dass der Austausch mit den betrieblichen Datenschutzbeauftragten für meine Arbeit sehr wichtig ist und auch bleibt. 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 für - u. U. auch problematische - Themen, auf die ich nur ungern verzichten möchte. 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 auch meinen Beitrag zu leisten.

Im Berichtsjahr wurde über folgende Themen diskutiert (Auszug):

- Umfang des Rechts auf Auskunft
- Rechtsstellung und Aufgaben des betrieblichen Datenschutzbeauftragten
- Aufbewahrungsfristen
- Datenschutzmanagementsysteme
- Auftragsverarbeitung bei der Baden-Badener Pensionskasse
- Cookie-Banner/Consent-Managementsysteme
- Zusammenarbeit mit der AG Datenschutz der Juristischen Kommission der Rundfunkanstalten
- Schmerzensgeld wegen unvollständiger Auskunft
- M365 und MS-Teams
- DSGVO konforme Vergabe/Beschaffung
- SAP
- Einsatz von KI/ChatGPT
- Beschaffung digitales Hinweisgebersystem

8.2 Empfehlungspapier Datenschutzmanagementsystem

Das Thema Datenschutzmanagement ist eine zentrale Aufgabe der Verantwortlichen zur Herstellung einer Datenschutz-Compliance. Einfach ausgedrückt wird mit einem solchen System

sichergestellt, dass sämtliche datenschutzrechtlichen Pflichten eingehalten, die verantwortlichen und handelnden Personen entsprechend benannt und geschult sowie die dahinterstehenden Prozesse definiert sind. Es handelt sich also um eine Managementaufgabe, die auch anhand einer Risikoanalyse der Verarbeitungen sämtliche Prozesse und Verantwortlichkeiten innerhalb ihres Bereiches definiert, damit die datenschutzrechtlichen Regelungen umgesetzt werden. Dazu gehört neben einer Dokumentation aller Verarbeitungstätigkeiten in einem Verzeichnis auch die Erstellung von Musterprozessen zum Umgang mit Datenschutzverletzungen, zur Erfüllung der Betroffenenrechte und zur Umsetzung von Auftragsverarbeitungsvereinbarungen sowie zur Erstellung von Risikoanalysen von Verarbeitungen und der daraus folgenden Datenschutzanforderungen.

Der AK DSB hat im Berichtsjahr unter meiner Mitwirkung eine Empfehlung für ein Datenschutzmanagementsystem erarbeitet, in der in angemessener und ausführlicher Art und Weise die Eckpunkte eines solchen Systems definiert werden. Dieses Papier erlaubt es, die bereits vorhandenen Prozesse in den einzelnen Rundfunkanstalten zu überprüfen und ggf. Defizite aufzuarbeiten. Wo ggf. noch kein Datenschutzmanagementsystem formell etabliert ist, gibt diese Empfehlung eine sehr gute Handreichung, wie ein solcher Prozess oder ein solches Projekt zur Umsetzung eines solchen Systems angegangen werden kann.

Im Jahr 2024 habe ich bereits begonnen, im Rahmen von regelmäßigen Gesprächen, den Umsetzungsstand des Datenschutzmanagements in den einzelnen Rundfunkanstalten zu untersuchen. Ich plane dies auszuweiten und werde darüber berichten.

9 Zusammenarbeit mit den Aufsichtsbehörden

9.1 Austausch mit der Datenschutzkonferenz (DSK)

Das Bundesdatenschutzgesetz sieht vor, dass die Datenschutzaufsichtsbehörden der Länder und ebenso der Bundesdatenschutzbeauftragte in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der DSGVO zusammenarbeiten. In diesem Zusammenhang sind auch die nach den Art. 85 und 91 der DSGVO eingerichteten Aufsichtsbehörden zu beteiligen. Ausgehend von dieser Vorschrift treffen Vertreter und Vertreterinnen des Bundesdatenschutzbeauftragten, der Landesdatenschutzbeauftragten mit den Rundfunkdatenschutzbeauftragten, den Aufsichten über den privatrechtlichen Rundfunk sowie den Aufsichten über die evangelische und katholische Kirche zusammen.

Diese Treffen fanden im Berichtsjahr 2023 am 21. Juni und am 28. November statt. Turnusgemäß wird aus der Datenschutzkonferenz berichtet und aus dem Europäischen Datenschutzausschuss. Ein stetig wiederkehrendes Thema ist die Verbesserung der Kooperation zwischen der DSK und den sogenannten „spezifischen“ Aufsichtsbehörden. Bereits in meinem letzten Bericht (dort Kapitel 9.1.) habe ich ausführlich über das Positionspapier der Rundfunkdatenschutzkonferenz zur Zusammenarbeit mit der DSK berichtet. Seitdem hat sich aber nichts Wesentliches verändert, insbesondere ist die frühzeitige Einbindung in die wichtigen Themen nur eingeschränkt gewährleistet.

In der Sitzung im November 2023 wurde vom Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland (EKD) die Bitte vorgetragen, ob und inwieweit Vertreter der evangelischen und der katholischen Kirche in der DSK gastweise mitarbeiten dürfen. Ich habe mich diesem Wunsch angeschlossen und bekräftigt, dass die Rundfunkdatenschutzbeauftragten als Aufsichtsbehörden grundsätzlich in der DSK ihren Platz finden sollten. In diesem Zusammenhang wurde erneut darauf hingewiesen, dass die Aufsichtsbehörden des Rundfunks und der Kirchen erst zum Zeitpunkt der Veröffentlichung von Beschlüssen und Entschließungen der DSK Kenntnis von diesen erlangten und nicht daran mitarbeiten dürften. Daher stellte sich die grundsätzliche Frage, inwieweit diese Beschlüsse auch für die nicht daran beteiligten Aufsichtsbehörden gelten können.

Ich bin gemeinsam mit dem Rundfunkdatenschutzbeauftragten des NDR der Meinung, dass ein Gaststatus sowohl in den ausgewählten Arbeitskreisen als auch in der DSK selbst erreicht werden müsste. Daher habe ich mich mit Schreiben vom 14.12.2023 an die Vorsitzende der DSK, die Landesbeauftragte für Datenschutz Schleswig-Holstein, Frau Dr. Marit Hansen, gewandt und unter Hinweis auf das Positionspapier der RDSK zur Zusammenarbeit den nationalen Aufsichtsbehörden vom Juli 2021 folgende Vorstellungen formuliert:

- Einräumung eines Gaststatus für einen Vertreter der RDSK im Rahmen der DSK
- Mitarbeit im AK Medien, dem AK Grundsatz und dem AK Technik, wobei sämtliche Beratungsunterlagen und der vorbereitende Schriftverkehr vollständig übermittelt werden
- Vereinbarung von Kriterien für Angelegenheiten, in denen eine engere Einbindung wünschenswert ist, mindestens aber ein Verfahren zur Identifikation solcher Fälle

Ich habe den Eindruck bekräftigt, dass eine Einbeziehung der sogenannten „spezifischen“ Aufsichtsbehörden eher zufällig erfolge und insbesondere eine thematische Abstimmung nicht stattfinde. Ich habe zudem betont, dass dies zumindest bei Medienthemen erforderlich wäre, was sich aus der Natur der Sache ergäbe.

Bis zum Redaktionsschluss dieses Tätigkeitsberichtes ist keine Antwort der DSK zu diesem Schreiben eingegangen.

9.2 AK Medien

Eine Teilnahme an der Sitzung des AK Medien am 18./19.09.2023 war geplant, konnte jedoch wegen technischer Probleme nur ausschnittsweise mitverfolgt werden.

Ein Schwerpunkthema war die Ansprache von Kindern über Social Media/Facebook durch öffentliche Stellen. Es wurde darüber debattiert, wie eine datenschutzkonforme Nutzung von Social Media durch Kinder und Jugendliche möglich sein kann.

Ein weiteres Thema war der Umgang mit dem Google-Firebase SDK (Software Development Kit) und die Frage, ob die Verbindung zu Google und dessen Server in den USA als „ausdrücklich gewünscht und damit erforderlich“ im Sinne von § 25 Abs. 2 Nr. 2 TTDSG sei. Hier bestand Uneinigkeit über die Wertung, vertreten wurde aber auch, dass im Zweifel ein anderes SDK genutzt werden solle.

9.3 AK Grundsatz

An der Sitzung des AK Grundsatz am 18./19.10.2023 in Bonn habe ich teilgenommen. Im Zuge dieser Sitzung wurden verschiedene grundsätzliche Themen zur Ausprägung und Anwendung der DSGVO behandelt. Berichte aus den subgroups des EDSA sind stets vorgesehen; ebenso wurde eine Diskussion zur der Frage geführt, wann ein Interessenskonflikt eines betrieblichen Datenschutzbeauftragten nach Art. 38 Abs. 6 DSGVO vorliegt und über spezielle Ausgestaltungen von Auftragsverarbeitungsverträgen debattiert.

Ohne auf einzelne Themen weiter einzugehen, möchte ich meinen Eindruck schildern, dass der persönliche Austausch in diesem Arbeitskreis von mir als sehr bereichernd empfunden wurde. Insofern halte ich es auch aufgrund dieser Erfahrung für wichtig, mit den Datenschutzbeauftragten der Länder und des Bundes enger zusammenzuarbeiten, was den Wunsch nach einer Mitgliedschaft in der Datenschutzkonferenz (wenn auch nur als Gast) unterstreichen soll.

10 Schlussbemerkungen und Ausblick

Das erste Jahr meiner Tätigkeit als Aufsichtsbehörde über insgesamt neun Rundfunkanstalten liegt nun hinter mir und uns. Es hat sich gezeigt, dass viele neue Herausforderungen zu bewältigen waren und neun Rundfunkanstalten nun mal mehr sind als eine oder zwei. Dies bedeutet auch, dass es notwendig war, die Aufgaben im Hinblick auf sinnvolle Schwerpunkte abzuschichten und neu zu sortieren. Insbesondere hat sich gezeigt, dass der Blick in die einzelnen Themen und Herausforderungen der Landesrundfunkanstalten, des ZDF und von Deutschlandradio nicht in der von mir zunächst ins Auge gefassten Tiefe und Präzision möglich gewesen ist. Dafür fehlten schlicht Ressourcen – insbesondere in Ansehung des hohen Beschwerdeaufkommens.

Dennoch soll dieses Ziel nicht aus den Augen verloren werden. Mit vier festen Terminen pro Jahr und Rundfunkanstalt soll der Blick geschärft und die Aufgabe als Aufsicht nuanciert werden. Dies wird und ist bereits möglich durch personellen Zuwachs in meiner Behörde ab dem 01.01.2024: Ich konnte mit einer zusätzlichen Referentin eine Mitarbeiterin gewinnen, die sich insbesondere technischen und organisatorischen Fragen - sowohl im Datenschutz als auch in der innerbehördlichen Organisation - widmen wird. Dadurch sollte es meiner Einschätzung nach möglich sein, die Prozesse effektiver zu gestalten und intensiver in Themen der jeweiligen Rundfunkanstalten hineinzusehen. Im nächsten Tätigkeitsbericht werde ich berichten, ob dieses Ziel erreicht werden konnte.

Was aber soll konkret getan werden? Angeklungen ist bereits, dass ich ein Audit der Apps der Rundfunkanstalten plane, was ggf. im Jahr 2024, jedoch in jedem Fall im Jahr 2025 angegangen wird. Themen, die uns weiterhin beschäftigen werden, sind Anwendungen der Künstlichen Intelligenz und die stets aufs Neue herauffordernde Abgrenzung und Definition von Verarbeitungstätigkeiten, die aufgrund ihrer journalistischen Prägung vom Medienprivileg umfasst sind. Ebenso plane ich, Anschlussprüfungen im Hinblick auf eine Querschnittsuntersuchung bei den Beteiligungsunternehmen und GSEAs der Rundfunkanstalten in Angriff zu nehmen sowie die Verzeichnisse der Verarbeitungstätigkeiten zumindest stichprobenartig anzuschauen. Wichtig ist - und aus meiner Sicht in den letzten Jahren stets ein bisschen vernachlässigt - der Redaktionsdatenschutz. Wegen des die journalistische Datenverarbeitung fast vollständig vom Anwendungsbereich der DSGVO trennenden Medienprivilegs kann der Eindruck entstehen, dass journalistische Datenverarbeitung ohnehin vom Datenschutz nicht in den Blick genommen wird. Dies ist einerseits richtig, andererseits aber auch nicht, denn das Datengeheimnis und damit die strenge Zweckbindung der journalistischen Datenverarbeitung muss in jedem Fall sichergestellt werden. Ich habe mir daher die Aufgabe gestellt zu prüfen, wie mit Daten in Redaktionen umgegangen wird, wie dort die Prozesse gestaltet sind und wie insbesondere sichergestellt wird, dass sensible Journalisten-Daten (Stichwort Informantenschutz) in angemessener Art und Weise

unter Sicherheitsgesichtspunkten behandelt werden. Auf diese Aufgabe bin ich besonders gespannt, da dies einen Einblick in die Welt der Redaktionen eröffnen dürfte.

Der Einsatz von M365 von Microsoft bleibt problematisch. Die staatlichen Aufsichten sehen Schwierigkeiten insbesondere wegen der nicht immer transparenten Vertragsgestaltung, bei Unklarheiten hinsichtlich der Nutzung von Daten aus der Auftragsverarbeitung für eigene Zwecke Microsofts und hinsichtlich der mangelnden Einwirkungsmöglichkeiten der Auftraggeber. Dies stellt die Verantwortlichen der diese Software einsetzenden Rundfunkanstalten vor Herausforderungen. Die Rundfunkanstalten bemühen sich um einen Austausch mit Microsoft, um die Probleme zu lösen und einen rechtssicheren Einsatz zu ermöglichen. Ich werde Anstrengungen unternehmen, den Austausch mit den staatlichen Aufsichtsbehörden zu dem Thema voranzutreiben und Lösungen zu unterstützen. Allerdings wird es mir nicht möglich sein, einzelne Software-Produkte vollumfänglich zu überprüfen, was in meinen Augen ohnehin nicht Aufgabe einer Aufsicht ist. Dessen ungeachtet darf dieses Thema nicht aus den Augen verloren werden.

Ich darf mich bei allen Rundfunkanstalten, den Rundfunk-, Fernseh- und Hörfunkräten, den Verwaltungsräten und auch den Geschäftsleitungen sehr herzlich bedanken für das mir entgegengebrachte Vertrauen und der Hoffnung Ausdruck verleihen, dass auch die kommenden Jahre der Zusammenarbeit ebenso erfolgreich wie vertrauensvoll verlaufen werden. Ich mache die Arbeit nach wie vor sehr gern und stelle mich den Herausforderungen. Datenschutz - dies hat sich in den Jahren meiner Tätigkeit gezeigt - birgt immer wieder Überraschungen und bleibt in jeden Fall spannungsreich und dynamisch.

11 Anhang

11.1 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.

11.2 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.

11.3 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.

11.4 TTDSG § 25

§ 25 TTDSG

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) 2016/679 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 Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

11.5 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.

11.6 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

11.7 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 25.01.2024

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

Hamburg, den 30.01.2024

Der Rundfunkdatenschutzbeauftragte beim NDR

Bremen, den 14.02.2024

Die Beauftragte für den Datenschutz bei Radio Bremen

Bonn, den 14.2.2024

Der Beauftragte für den Datenschutz der Deutschen Welle

4

Anlage zur
Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen und über Gemeinschaftsunternehmen der Rundfunkanstalten
Stand: Dezember 2023

	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, 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