Der Rundfunkdatenschutzbeauftragte

ARD · ZDF · Deutschlandradio

TÄTIGKEITS BERICHT

25

Der Rundfunkdatenschutzbeauftragte

ARD · ZDF · Deutschlandradio

Stephan Schwarze

Kantstraße 71-73, 04275 Leipzig

www.rundfunkdatenschutz.de

Leipzig, Mai 2026

Berichtszeitraum: 01.01.2025 bis 31.12.2025

Inhaltsverzeichnis

Vorwort 7

1 Einleitung 9

2 Aufgaben und Befugnisse des Rundfunkdatenschutzbeauftragten 9

2.1 Gesetzliche Grundlagen 10

2.2 Aufgabe und Unabhängigkeit – ein Beispiel 11

2.3 Zuständigkeit bei Rechtsverletzungen durch Berichterstattung 12

2.4 Vorstellung meines Tätigkeitsberichts 2024 im Sächsischen Landtag 13

3 Entwicklungen im Datenschutzrecht 15

3.1 Medienstaatsvertrag 16

3.2 Wirksamwerden der KI-VO 16

3.3 NIS2-Richtlinie 17

3.4 Einwilligungsverwaltungsverordnung (EinwV) 18

3.5 Digitaler Omnibus – geplante Änderungen DSGVO 19

3.6 EDSA-Stellungnahmen und Leitlinien 22

3.6.1 Leitlinien zur Pseudonymisierung 22
3.6.2 Leitlinien zum Zusammenspiel von DSA und DSGVO 23
3.6.3 Gemeinsame Leitlinie von EDSA und Europäischer Kommission zu DMA und DSGVO 23

3.7 Rechtsprechung 24

3.7.1 Negative Gefühle als immaterieller Schaden – Voraussetzung des Kontrollverlustes 24
3.7.2 Klage auf Nichtigerklärung des EU-Angemessenheitsbeschlusses (Urteil des EuG) 26
3.7.3 EuGH präzisiert Begriff der personenbezogenen Daten 26
3.7.4 Facebook-Fanpages 28
3.7.5 Datenschutzrechtliche Verantwortlichkeit von Arbeitnehmern 28

4 Eingaben beim Rundfunkdatenschutzbeauftragten 29

4.1 Beschwerden 30

4.2 Sonstige Eingaben 31

4.3 Entwicklung der Eingaben 2023 bis 2025 32

4.4 Klagen und Gerichtsverfahren 34
4.5 Dienstaufsichtsbeschwerde 34

5 Meldungen nach Art. 33 DSGVO 35
5.1 Meldeeingänge 36
5.2 Entwicklung der Meldungen 2023-2025 37
5.3 Verbesserungsbedarf bei Meldungen nach Art. 33 DSGVO 38
5.3.1 Kommunikation mit der Aufsichtsbehörde 38
5.3.2 Risikobewertung nach Art. 34 DSGVO 39
5.3.3 Betroffeneninformation 39

6 Themen und Schwerpunkte der Aufsicht 40
6.1 Prüfungen 40
6.1.1 Befragung zu Onboarding und Schulung 40
6.1.2 Befragung zum Redaktionsdatenschutz 42
6.1.3 Geplante Prüfungen für das nächste Berichtsjahr 48
6.2 Handreichung zu Aufbau und Weiterentwicklung eines DSMS 48
6.3 Aufzeichnung von Personalversammlungen 49
6.4 Datensicherheit in der Aufsichtstätigkeit 50
6.5 Notwendigkeit einer Wiederholung der Verpflichtung auf das Datengeheimnis? 52
6.6 WhatsApp als Kommunikationsweg 53
6.7 Sammelbeschwerde Videoüberwachung 54
6.8 Künstliche Intelligenz 55
6.9 Medienprivileg 57
6.9.1 Rechtsgrundlagen und Anwendbarkeit des Medienprivilegs 58
6.9.2 Was erreichte uns zum Medienprivileg? 59
6.9.3 Auskunftsanspruch und Medienprivileg 59
6.9.4 Unberechtigte Weitergabe von personenbezogenen Daten 62
6.9.5 Speicherung und Verarbeitung von Interviewdaten bei Straßenumfragen 63
6.10 Übertragung zusätzlicher Aufgaben an den Datenschutzbeauftragten 64
6.11 Private Nutzung dienstlicher Kommunikationswege (Mitarbeiterexzess) 65
6.12 Internationale Zusammenarbeit zwischen Aufsichtsbehörden 66

7 Datenschutz in den Rundfunkanstalten 67
7.1 Einführung bzw. Weiterentwicklung eines Datenschutzmanagementsystems 67
7.2 Kennzahlen zu Eingabebearbeitung und Datenschutzvorfällen 68
7.3 Datenschutzrechtliche Themenschwerpunkte 69
8 Datenschutz beim Beitragsservice 69
8.1 Fragwürdiger Service für Rundfunkbeitragsangelegenheiten 70
8.2 Konzertierte Aktion gegen den Beitragsservice 71
8.3 Sorgt KI für eine Beschwerdeflut? 72
8.4 Abgrenzung Datenschutzrecht und Beitragsrecht 72
8.5 Datenübermittlung nach § 11 Abs. 4 Rundfunkbeitragsstaatsvertrag 73
9 Rundfunkdatenschutzkonferenz (RDSK) 74
9.1 Aufgaben der RDSK 74
9.2 Handreichungen, Empfehlungen und Orientierungshilfen 75
9.2.1 Stellungnahme zur Informationsplicht des Verantwortlichen über Auftragsverarbeiter und Unterauftragsverarbeiter im Sinne von Art. 28 DSGVO 76
9.2.2 Empfehlungen zum Umgang mit dem Data Privacy Framework (DPF) – Version 2.0 mit Hinweisen zur Digitalen Souveränität 77
10 Austausch mit dem Arbeitskreis der Datenschutzbeauftragten (AK DSB) 79
11 Austausch mit der Datenschutzkonferenz (DSK) 79
11.1 AK Medien 81
11.2 AK Grundsatz 82
11.3 AK Technik 82
11.4 AK KI 83
12 Ausblick und Schlussbemerkung 84
13 Anhang 86
13.1 DSGVO Art. 51 ff. 86
13.2 DSGVO Art. 85 91
13.3 MStV – §§ 12, 23, 31j ff., 113 92

13.4 TDDDG § 25 96

13.5 RDSK-Mitgliederliste 2025 97

13.6 RDSK-Verwaltungsvereinbarung 98

Vorwort

Im Vorwort zu meinem letztjährigen Tätigkeitsbericht habe ich den Begriff „ruhiges Fahrwasser“ benutzt und damit zum Ausdruck gebracht, dass Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk dynamisch und vielfältig ist und damit kaum so charakterisiert werden kann – daran hat sich nichts geändert. 2025 lässt sich als ein Jahr einordnen, in dem vieles gleichzeitig in Bewegung geraten ist – rechtlich wie auch organisatorisch.

Letzteres insbesondere deshalb, weil meine Aufsichtsbehörde vor der Herausforderung stand, ihr Aktenmanagementsystem auf eine neue Plattform umzustellen, was sich als zeitaufwendig und in Teilen sehr schwierig erwiesen hat.

In den letzten Monaten des Berichtsjahres hat sich eine enorme Steigerung des Beschwerdeaufkommens abgezeichnet. Dies ist eine Entwicklung, die nach übereinstimmender Wahrnehmung auf den Vormarsch der Künstlichen Intelligenz zurückzuführen ist. Die staatlichen Datenschutz-Aufsichtsbehörden melden Anstiege bei den Beschwerden von 60% bzw. 90%. Dies zeigt sich aktuell auch in meiner Behörde: Von Januar bis Ende März 2026 sind bereits mehr als doppelt so viele Eingaben eingegangen wie im Vorjahr.

Auch die Zahl der gemeldeten Datenschutzvorfälle steigt aktuell deutlich. Dies kann einerseits darauf hindeuten, dass zunehmend auch KI-gestützte Angriffsmethoden eingesetzt werden, insbesondere im Bereich von Phishing-Kampagnen und dem gezielten Kompromittieren von Benutzerkonten. Andererseits ist zu berücksichtigen, dass in den Rundfunkanstalten eine gestiegene Sensibilität für Datenschutzvorfälle zu beobachten ist, die sich in einer konsequenteren Erkennung, Bewertung und Meldung entsprechender Sachverhalte niederschlägt.

Das Thema Künstliche Intelligenz muss weiterhin aus datenschutzrechtlicher Perspektive im Auge behalten werden. Im Januar des Berichtsjahres wurde der Arbeitskreis KI der Datenschutzkonferenz ins Leben gerufen, an dem meine Behörde als Gast beteiligt ist. Ein erklärtes Ziel war es überdies, die vielfältigen Entwicklungen und Einsatzgebiete der KI im öffentlich-rechtlichen Rundfunk zu überblicken. Dies war im Berichtsjahr aufgrund der rasanten Entwicklungen und begrenzten Ressourcen nicht im gewünschten Maße möglich.

Eine sichtbare Kursmarke des Jahres 2025 war und ist der als Reformstaatsvertrag bezeichnete 7. Medienänderungsstaatsvertrag. Die Regierungschefinnen und Regierungschefs der Länder haben den Staatsvertrag im März 2025 unterzeichnet, er wurde von allen Landesparlamenten ratifiziert und ist zum 01. Dezember 2025 in Kraft getreten. Damit werden Auftrag, Organisation und Zusammenarbeit von ARD, ZDF und Deutschlandradio spürbar modernisiert – von einer verbindlichen Kooperation über die Plattform- und Portfoliostrategie bis hin zu Effizienz- und Kontrollmechanismen.

Mit der Reform der staatsvertraglichen Regeln ging ebenso eine tiefgreifende Änderung der strukturellen und rechtlichen Anbindung der Rundfunkdatenschutzaufsicht einher. Der Staatsvertrag sieht nunmehr eine gemeinsame Aufsicht vor, die für alle Landesrundfunkanstalten, das ZDF und Deutschlandradio sowie deren Beteiligungsunternehmen zuständig ist. Damit ist eine bundesweit zuständige Behörde geschaffen worden, deren Bedeutung, Verantwortung und Aufsichtsumfang weit über die bisherigen Regelungen hinausweist, wonach jede Anstalt einen eigenen Rundfunkdatenschutzbeauftragten zu ernennen hatte. Der Neugestaltung der Aufsicht wurde in den vergangenen Jahren insoweit vorgegriffen, als dass sich sieben Rundfunkanstalten, das ZDF und Deutschlandradio bereits darauf geeinigt hatten, einen (gemeinsamen) Rundfunkdatenschutzbeauftragten zu bestellen, der für alle an diesem Modell Beteiligten zuständig war. Mit den Regelungen im Medienstaatsvertrag werden die institutionellen Leitplanken der Tätigkeit nunmehr gesetzlich und einheitlich verankert – einschließlich Zuständigkeit, Unabhängigkeit und Ausstattung des gemeinsamen Rundfunkdatenschutzbeauftragten. Die §§ 31j ff. MStV sind insoweit eindeutig und ebenso die gemeinsame Satzung der Rundfunkanstalten, die im Hinblick auf die Satzungsermächtigung des § 31j MStV bereits von sämtlichen ARD-Landesrundfunkanstalten, dem ZDF und Deutschlandradio beschlossen wurde.

Nach wie vor sehe ich es als zentrale Aufgaben an, Datenschutzüberprüfungen und Audits durchzuführen, sowie Beschwerden und Anfragen aus den Anstalten zu bearbeiten. Es gibt daneben viele interessante und spannende Themen, die aufzugreifen sich lohnen würde – allein die begrenzten Ressourcen stehen der Umsetzung entgegen.

Im Bericht finden sich die Entwicklungen zum Datenschutzrecht und auch die wichtigsten Urteile. Ausgewählte Aktivitäten meiner Aufsichtsbehörde werden ausführlich beleuchtet und wie immer wird der Versuch unternommen, ein anschauliches Bild meiner Aufgaben zu zeichnen, das gut lesbar und auch für den interessierten Laien verständlich sein soll.

Auch im Berichtsjahr 2025 wurde ich unterstützt von einer Referentin, einem Referenten und einer Assistentin, die in vorbildlicher Weise und mit sehr viel Einsatz die Arbeit der Aufsichtsbehörde erst möglich gemacht haben. Ihnen gebührt mein herzlicher und uneingeschränkter Dank.

Ich freue mich, in diesem Bericht über interessante Themen berichten zu können. Wie immer wünsche ich allen Leserinnen und Lesern eine kurzweilige und aufschlussreiche Lektüre und wiederhole mich in dem Wunsch, dass Datenschutz als interessant und lebensnah wahrgenommen wird.

Leipzig, im Mai 2026
Stephan Schwarze

1 Einleitung

Nach § 31l Abs. 4 Medienstaatsvertrag legt der Rundfunkdatenschutzbeauftragte als Aufsichtsbehörde einen Jahresbericht über seine Tätigkeit vor. Im Berichtsjahr hatte diese Vorschrift noch keine Geltung, denn sie bezieht sich auf den gemeinsamen Rundfunkdatenschutzbeauftragten nach dem Reformstaatsvertrag, der erst im Dezember des Berichtsjahres in Kraft getreten ist. Die für die bisherige gemeinsame Aufsicht über sieben Rundfunkanstalten, das ZDF und Deutschlandradio maßgeblichen Vorschriften sehen vor, dass ich diesen Bericht den Organen zur Verfügung zu stellen habe[1]. Dies sind die Verwaltungsräte, die Rundfunk-, Hörfunk- oder Fernsehräte sowie die Intendantinnen und Intendanten, die ich förmlich über meinen Bericht unterrichte. Meiner Veröffentlichungspflicht komme ich nach, indem ich den Bericht auf meiner Website www.rundfunkdatenschutz.de zur Verfügung stelle. Die jeweiligen Landesregierungen und Parlamente, darunter die für das ZDF und das Deutschlandradio jeweils aktuell rechtsaufsichtsführenden Länder, werden ebenfalls von der Veröffentlichung des Berichts in Kenntnis gesetzt.

2 Aufgaben und Befugnisse des Rundfunkdatenschutzbeauftragten

Der neue Medienstaatsvertrag, gültig seit dem 01.12.2025, legt fest, dass es nunmehr einen gemeinsamen Rundfunkdatenschutzbeauftragten für die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF und Deutschlandradio sowie die von ihnen verantworteten Gemeinschaftseinrichtungen und ihre Beteiligungsunternehmen gibt. Dieser gemeinsame Rundfunkdatenschutzbeauftragte ist die einzig zuständige unabhängige Aufsichtsbehörde über den öffentlich-rechtlichen Rundfunk in Deutschland. Bereits seit dem Jahr 2023 nehme ich gemeinsam für BR, hr, MDR, rbb, SR, SWR, WDR, ZDF und Deutschlandradio diese Aufsicht wahr; hinzugekommen sind durch die staatsvertragliche Regelung Radio Bremen und der Norddeutsche Rundfunk sowie die Aufsicht über den nicht-journalistischen Bereich des Hessischen Rundfunks. In diesem Kapitel wird über die Besonderheiten der gemeinsamen Aufsicht sowie den gesetzlich zugewiesenen Aufgaben informiert.

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

2.1 Gesetzliche Grundlagen

Der nach der bisherigen, im Berichtsjahr geltenden Rechtslage 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 erfolgte bisher die Ernennung für die Dauer von vier Jahren, beim Saarländischen Rundfunk und beim Südwestrundfunk für die Dauer von sechs Jahren. Das Amt des Rundfunkdatenschutzbeauftragten war und ist unabhängig ausgestaltet, er unterliegt insbesondere keiner Rechts- oder Fachaufsicht. Beim BR, MDR, rbb, WDR, Deutschlandradio und ZDF war bislang geregelt, dass die vom Verwaltungsrat ausgeübte Dienstaufsicht diese Unabhängigkeit keinesfalls beeinträchtigen darf. Nach § 27 Abs. 5 Landesdatenschutzgesetz Baden-Württemberg unterlag der Rundfunkdatenschutzbeauftragte beim SWR im Gegensatz dazu keiner Dienstaufsicht. Gemäß § 28 Abs. 2 Hessisches Datenschutz- und Informationsfreiheitsgesetz überwachte der Rundfunkdatenschutzbeauftragte den Datenschutz im journalistischen Bereich frei von Weisungen. Damit war auch nach der alten Rechtslage die Unabhängigkeit in vollständiger Weise umgesetzt.

Mit Inkrafttreten des neuen Medienstaatsvertrages wurde die Aufsicht gebündelt, so dass ab dem Jahr 2026 die Landesvorschriften keine Wirkung mehr entfalten. An der Unabhängigkeit und auch an den Aufgaben der Aufsicht hat sich indes nichts geändert. Die maßgeblichen Vorschriften zu Ernennung, Unabhängigkeit und Aufgaben finden sich in den §§ 31j ff. MStV.

In seiner Funktion als Aufsichtsbehörde ist der Rundfunkdatenschutzbeauftragte zuständig für die Überwachung der Einhaltung des Datenschutzes in den Rundfunkanstalten[2] bei ihren gesamten Tätigkeiten, einschließlich der 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 eines ihrer Beteiligungsunternehmen in ihren oder seinen Rechten verletzt worden zu sein. Hinzu kommen die Aufgaben nach Artikel 57 DSGVO, wonach insbesondere die Datenschutzgrundverordnung zu überwachen und durchzusetzen ist. Dort ist auch geregelt, dass der Rundfunkdatenschutzbeauftragte an der Sensibilisierung der Verantwortlichen, der betroffenen

[2] Deutschlandradio ist eine Körperschaft, der Einfachheit halber wird in diesem Bericht allein von Rundfunkanstalten gesprochen.

Personen und der Öffentlichkeit mitzuwirken hat und mit anderen Aufsichtsbehörden zusammenarbeiten soll.

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

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

2.2 Aufgabe und Unabhängigkeit – ein Beispiel

Zur Verdeutlichung der Aufgabe und der Unabhängigkeit mag ein Fall dienen, mit dem ich mich im Berichtsjahr zu befassen hatte: Er ist insoweit interessant, weil er ein Licht auf die Wahrnehmung des Rundfunkdatenschutzbeauftragten wirft.

Es ging darum, ob Interessensvertretungen Zugriff auf bestimmte Prüfberichte haben dürfen. Es wurde die Auffassung vertreten, dass die Geschäftsleitung einer Landesrundfunkanstalt ihre datenschutzrechtlichen Bedenken hinsichtlich der Verweigerung der Weitergabe eines Untersuchungsberichtes nicht hinreichend begründet habe, und dass die Rundfunkdatenschutzaufsicht dies anhand von vorgelegten Unterlagen beurteilen können müsste.

Ich habe auf folgende Umstände hingewiesen: Der Rundfunkdatenschutzbeauftragte vertritt als völlig unabhängige Aufsichtsbehörde weder Interessen noch schließt er sich a priori einer Meinung an. Daher ist er verpflichtet, im Rahmen des Amtsermittlungsgrundsatzes alle Hintergründe einer Anfrage und auch die Auffassung aller beteiligten Bereiche einer Rundfunkanstalt zu ermitteln. Die Behörde hat nachzuvollziehen, welcherlei personenbezogene Daten betroffen sind und insbesondere auch, ob die Kenntnis dieser Daten von der anfordernden Stelle zur Erfüllung ihrer Aufgaben benötigt wird. Nicht zu entscheiden hat sie indes, ob die Sachinformationen eines solchen

Berichtes zweckdienlich oder angemessen sind, sondern nur, ob die personenbezogenen Daten, die ein solcher Bericht beinhaltet, durch die anfordernde Stelle zur Kenntnis genommen und verarbeitet werden dürfen. In Ansehung der Aufgaben der anfordernden Stelle ist zu bewerten und zu klären, ob sie ihren Aufgaben nur dann nachkommen kann, wenn die streitigen Daten vorliegen.

Im Rahmen der Prüfung der Erforderlichkeit muss abgewogen werden zwischen einer Aufgabe, die im öffentlichen Interesse liegt, für die es eine Rechtsgrundlage geben muss, und dem Recht der betroffenen Person(en) auf informationelle Selbstbestimmung. Ebenso zu prüfen sind alle weiteren relevanten Datenschutzaspekte, insbesondere die Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO und die Beachtung der Datensicherheit.

Da die Interessensvertretung in diesem Fall nicht wünschte, dass ich im Rahmen der Amtsermittlung an die Geschäftsleitung der Anstalt herantrete, um den gegenständlichen Bericht auf seine Datenschutzrelevanz zu prüfen, ist die Anfrage an meine Behörde nicht weiterverfolgt worden.

An diesem Beispiel wird deutlich, dass die Datenschutzaufsichtsbehörde weder Teil der Rundfunkanstalten noch Teil sonstiger Interessensvertretungen ist und sich ihre Entscheidungen allein an den rechtlichen Vorgaben orientieren. Ich betone: Die Datenschutzaufsicht auch im öffentlich-rechtlichen Rundfunk ist völlig unabhängig, nur dem Gesetz unterworfen und hat ihre Aufgaben nach pflichtgemäßem Ermessen zu erfüllen.

2.3 Zuständigkeit bei Rechtsverletzungen durch Berichterstattung

Im Berichtsjahr erreichten mich Beschwerden und Fragen dazu, inwieweit der Rundfunkdatenschutzbeauftragte für Beschwerden bei möglichen Verletzungen von Persönlichkeitsrechten zuständig ist, die aufgrund von Berichterstattungen der Rundfunkanstalten vermutet werden.

Stets weise ich darauf hin, dass die §§ 12 und 23 Medienstaatsvertrag auf Basis von Art. 85 DSGVO die journalistische Datenverarbeitung weitgehend von den sonstigen datenschutzrechtlichen Vorgaben freistellen (ausführlich zum Medienprivileg siehe Kapitel 6.9 dieses Berichtes und ebenso Tätigkeitsbericht 2024, Kapitel 6.7). Hintergrund ist, dass journalistische Tätigkeit nicht mehr sinnvoll auszuüben und die für eine funktionsfähige demokratische Gesellschaft essenziellen Funktionen von Presse und Rundfunk ausgeschaltet wären, würden die allgemeinen Datenschutzregeln uneingeschränkt für diesen Bereich gelten. Folgerichtig ergibt sich aus der Systematik auch, dass in diesem Bereich die Datenschutzaufsicht nur untergeordnet bzw. in Teilaspekten, wie etwa der Datensicherheit und dem Datengeheimnis, zuständig ist. Ich weise auch stets darauf hin, dass die Rundfunkanstalten nicht völlig frei darin sind, ob und inwieweit sie z. B. in

identifizierender Weise über Personen berichten. Auch die Rundfunkanstalten sind gehalten, dies nur im Rahmen der allgemeinen persönlichkeitsrechtlichen Grenzen zu tun, dies gehört zu ihrer journalistischen Sorgfaltspflicht.

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

Man erkennt an dieser Konstellation, dass diese Ausgestaltung auf den ersten Blick verwirrend sein kann, denn der Datenschutz lebt nach einer Persönlichkeitsverletzung im Zusammenhang mit den dazu gespeicherten Daten wieder auf.

2.4 Vorstellung meines Tätigkeitsberichts 2024 im Sächsischen Landtag

Im Sommer 2025 erreichte mich eine Einladung des Ausschusses für Wissenschaft, Hochschule, Medien, Kultur und Tourismus des Sächsischen Landtages mit der Bitte, meinen Tätigkeitsbericht des Jahres 2024 vorzustellen. In der Tat gehört es zu meinen Pflichten, meinen Tätigkeitsbericht auch den Länderparlamenten zur Verfügung zu stellen, dies ergibt sich direkt aus Art. 59 DSGVO. Insofern freue ich mich stets darüber, in den Landtagen Rede und Antwort stehen zu dürfen.

Die Einladung in den Sächsischen Landtag im Jahr 2025 wies insoweit eine Besonderheit auf, als dass im Vorfeld noch zahlreiche weitere Fragen übermittelt wurden, um deren Beantwortung im Rahmen der Sitzung gebeten wurde. Diese Fragen hatten allerdings keinerlei Bezug zu meinem Tätigkeitsbericht, sondern wiesen eine andere Zielrichtung auf. Insbesondere wurden Fragen gestellt zu aus Sicht des Ausschusses fragwürdigem Verhalten des ZDF Magazin Royale und von Jan Böhmermann im Hinblick auf die Identität eines kritisierten YouTubers, und daran anknüpfend Fragen dazu, wie sich das Medienprivileg von mutmaßlichen Persönlichkeitsverletzungen abgrenzen lasse. Ebenso wurde die Berichterstattung des MDR thematisiert, die Gegenstand einer einstweiligen Verfügung des Landgerichts Berlin war. Auch hier wurde die Frage gestellt, inwieweit der Rundfunkdatenschutzbeauftragte einbezogen gewesen sei.

Ich bin in meinem Vortrag sehr ausführlich auf diese Fragen und das Medienprivileg eingegangen und habe verdeutlicht, dass es Zweck des Medienprivilegs sei, das Datenschutzrecht mit der Presse- und Rundfunkfreiheit in Einklang zu bringen. Durch die uneingeschränkte Geltung der allgemeinen Datenschutzregeln würde die für die Demokratie essenzielle Arbeit einer freien Presse und eines freien Rundfunks nicht ausreichend geschützt werden. Daher – so habe ich verdeutlicht – erfolgt im journalistischen Bereich die Datenschutzaufsicht lediglich im Hinblick auf Teilaspekte. Dazu gehört das Datengeheimnis, das die Zweckbindung der journalistischen Datenverarbeitung umschreibt. Betont habe ich auch, dass sich die kritisierten Fälle nicht auf meine Aufsichtszuständigkeit erstrecken.

Ich habe gleichwohl darauf hingewiesen, dass Medien nur im Rahmen der allgemeinen persönlichkeitsrechtlichen Sorgfaltspflichten über Personen berichten dürfen. Ebenso steht den betroffenen Personen der Gerichtsweg sowie der direkte Kontakt zu den Rundfunkanstalten offen. Die betroffenen Personen sind also nicht schutzlos, ihnen ist nur die Berufung auf das Datenschutzrecht in dieser Hinsicht verwehrt.

Auch der Vermutung, dass es sich bei der Berichterstattung des ZDF um eine Datenschutzverletzung nach Art. 33 DSGVO hätte handeln können, konnte ich entgegentreten. Nach gesetzlicher Definition ist dies eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung personenbezogener Daten führt. Eine – ggf. auch unrichtige oder unzulässige – Berichterstattung kann keine meldepflichtige Datenschutzverletzung sein, denn auch der Art. 33 DSGVO ist aufgrund des Medienprivilegs auf journalistische Datenverarbeitungen nicht anwendbar. Würden auch Beiträge, die in das Persönlichkeitsrecht eingreifen, als Datenschutzverletzung betrachtet, wäre das konträr zum Medienprivileg und der diesem Prinzip zugrunde liegenden freien Berichterstattung. Denn auch eine nach journalistischen Standards fehlerhafte Datenverarbeitung bleibt eine journalistische und kann damit nach dem Datenschutzrecht weder als zulässig noch als unzulässig bewertet werden. Ist eine Persönlichkeitsrechtsverletzung indes festgestellt, so kommt neben zivilrechtlichen Ansprüchen die Geltendmachung der Rechte nach den § 12 Abs. 3 und nach § 23 Abs. 2 Medienstaatsvertrag in Betracht.

Weitere Fragen bezogen sich auch auf die Speicherung personenbezogener Daten durch den WDR im Rahmen des Beitragseinzugs und diesbezügliche Löschungen. Ich habe darauf hingewiesen, dass beim Beitragsservice ein anforderungsgerechtes Löschkonzept existiert, und die konkrete Löschung beim Verantwortlichen liegt. Aufgabe der Datenschutzaufsichtsbehörde ist es, die Angemessenheit und Wirksamkeit der Löschregelungen zu kontrollieren, während eine Überprüfung einzelner Löschvorgänge nicht erfolgt.

Schließlich wurde ich dazu befragt, ob angesichts dieser Rechtslage meine Aufgabe als „Feigenblatt“ wahrgenommen werden müsse. Ich habe die Gelegenheit ergriffen, anhand von Beispielen (Überprüfung der Nutzungsmessung und Prüfung zum Redaktionsdatenschutz) zu verdeutlichen, dass meine Aufgaben vielfältig sind und die Themen zahlreich. Verwiesen habe ich auch auf die Datenverarbeitung zum Zwecke des Beitragseinzuges und darauf, dass die schiere Anzahl von Beitragskonten und die damit verbundene sehr große Menge von verarbeiteten Daten der besonderen Aufmerksamkeit durch die Aufsicht bedürften. Der ständige Austausch mit der behördlichen Datenschutzbeauftragten des Beitragsservice ist insoweit sichergestellt. Ich habe darüber hinaus auf meine Aktivitäten im Hinblick auf den Umgang mit Beschäftigtendaten, den Umgang mit Künstlicher Intelligenz und auch das Thema Drittstaatenübermittlung aufmerksam gemacht. Schließlich habe ich berichtet, dass aktuell das Thema Datenschutzmanagement von mir begleitet und überwacht wird.

Ich schätze es sehr, dass sich die politischen Akteure auch für den Rundfunkdatenschutz interessieren, stelle aber fest, dass bestimmte politische Richtungen offensichtlich die Rolle des Rundfunkdatenschutzbeauftragten insgesamt und auch seine gesetzlichen Aufgaben im Rahmen der medienprivilegierten journalistischen Datenverarbeitung infrage stellen. Ich bin aber jederzeit gern bereit, diese Fragen zu diskutieren und meine Rolle gegenüber den Landtagen oder anderen politischen Akteuren zu erläutern und die juristischen Hintergründe zu erklären.

3 Entwicklungen im Datenschutzrecht

Auch im Jahr 2025 prägten weitreichende gesetzgeberische Initiativen und neue europäische Regelungsentwürfe das Datenschutzrecht. Neben der stufenweisen Umsetzung der KI-Verordnung, die weiterhin im engen Zusammenspiel mit den datenschutzrechtlichen Vorgaben betrachtet werden muss, rückten zuletzt die geplanten Änderungen der DSGVO durch den Digitalen Omnibus in den Fokus. Zugleich wurden neue Pflichten im Bereich Cybersicherheit (NIS2-Umsetzung), digitaler Dienste (Einwilligungsverwaltungsverordnung) sowie im Zusammenspiel mit weiteren EU-Rechtsakten wie DSA und DMA konkretisiert. Ergänzend fanden wesentliche Leitlinien des Europäischen Datenschutzausschusses sowie bedeutende Entscheidungen der europäischen und nationalen Gerichte Eingang in die datenschutzrechtliche Diskussion. Der folgende Abschnitt gibt einen Überblick über diese Entwicklungen und deren Relevanz für die Rundfunkanstalten.

3.1 Medienstaatsvertrag

Der Medienstaatsvertrag (MStV) weist verschiedene neue bzw. vertiefende Anknüpfungspunkte zum Datenschutzrecht auf, die in der praktischen Umsetzung durch die Rundfunkanstalten berücksichtigt werden müssen. Hierbei handelt es sich im Schwerpunkt um folgende Themen:

- Umgang mit personenbezogenen Daten zum Zwecke der Auftragserfüllung, besondere Regeln als einheitlicher Standard (§ 31i MStV)
- Austausch personenbezogener Daten zwischen den LRAs, ZDF und Deutschlandradio auf Basis des gemeinsamen technischen Plattformsystems zur Verwirklichung des gemeinwohlorientierten Raums (§ 30f MStV)
- Datensichere und datensparsame Personalisierungsmöglichkeiten und Empfehlungssysteme mit einer öffentlich-rechtlichen Zielsetzung und Ausgestaltung; Auftrag der Anstalten zu mehr Interaktion mit den Rezipienten; Möglichkeiten der interaktiven Kommunikation (§ 30f MStV)
- Vernetzung der öffentlich-rechtlichen europäischen Partner (§ 30f MStV)
- Öffnung für und Zusammenarbeit mit privaten bzw. kommerziellen Anbietern (§§ 30d, 30f MStV)
- Nutzerzentrierte Angebote als Ausfluss des Auftrags; daran anknüpfend Fragen der Leistungsanalyse und entsprechender Datenverarbeitungen (§§ 26, 26a MStV)
- Gestaltung der Telemedienangebote und Berücksichtigung verschiedenster Zielgruppen, auch auf Drittplattformen (§ 30 MStV)
- Jugendangebot und die damit zusammenhängende Verarbeitung von Daten von Jugendlichen und Kindern (§ 30c MStV)

Hier wird es darauf ankommen, wie die Verantwortlichen diese Vorschriften umzusetzen gedenken, denn nur anhand der konkreten Verarbeitungen lässt sich eine datenschutzrechtliche Beurteilung vornehmen.

3.2 Wirksamwerden der KI-VO

Mit der Veröffentlichung der KI-Verordnung im Juli 2024 setzte die Europäische Union einen eigenständigen Rechtsrahmen für Künstliche Intelligenz. Die Umsetzung erfolgt stufenweise. Seit dem 02.02.2025 gelten bereits die ersten zentralen Bestimmungen, darunter das Verbot unzulässiger KI-Praktiken wie Social Scoring, invasive biometrische Echtzeitüberwachung und Systeme, die vulnerable Gruppen manipulieren. Gleichzeitig ist seit diesem Datum die Verpflichtung des Art. 4 KI-VO wirksam, wonach Anbieter und Betreiber die erforderliche KI-Kompetenz nachweisen müssen (siehe Kapitel 6.8). Art. 3 Nr. 56 KI-VO definiert diese als Fähigkeit, KI

sachkundig, risikobewusst und unter Kenntnis möglicher Schäden einsetzen zu können. Diese Kompetenzanforderung verlangt faktisch ein systematisches Verständnis der Funktionsweise von KI-Systemen, ihrer Risiken und der notwendigen Kontrollmechanismen – auch wenn die KI-VO selbst keine ausdrückliche Schulungspflicht vorsieht.

Für Rundfunkanstalten ergibt sich daraus ein unmittelbarer Handlungsbedarf: Sie müssen Strukturen schaffen, um ihr Personal sowohl technisch als auch datenschutzrechtlich zu befähigen. Der enge Zusammenhang zwischen KI-VO und DSGVO spielt hierbei eine wesentliche Rolle, da der Datenschutz weiterhin Anforderungen an Datenqualität, Transparenz und Zweckbindung stellt, während die KI-VO zusätzliche Pflichten wie Risikodokumentation und die Prüfung von Trainingsdaten auf Verzerrungen etabliert. Die von der RDSK entwickelte Orientierungshilfe[3] bietet hierfür bereits erste praxisnahe Leitlinien. Zu beachten ist zudem, dass eine unzureichende KI-Kompetenz im Haftungsfall als Sorgfaltspflichtverletzung bewertet werden kann.

Der August 2025 markierte den nächsten regulatorischen Meilenstein: Mit dem 02.08.2025 traten u. a. die Vorgaben für General-Purpose-AI-Modelle (GPAI) und Basismodelle in Kraft. Diese umfassen umfangreiche Transparenz- und Dokumentationspflichten, Risikobewertungen und Anforderungen an die Modellüberwachung, insbesondere bei potenziell systemischen Risiken. Auf nationaler Ebene wurde parallel der Entwurf zur Durchführung der KI-VO vorgelegt, einschließlich der Einrichtung eines Koordinierungs- und Kompetenzzentrums bei der Bundesnetzagentur, das eine einheitliche Rechtsauslegung sicherstellen soll.

Für den öffentlich-rechtlichen Rundfunk entsteht damit ein zunehmend verbindlicher Ordnungsrahmen: KI-Einsatz wird künftig nur dann rechts- und datenschutzkonform möglich sein, wenn Kompetenzen systematisch aufgebaut, Risiken nachweislich bewertet und die neuen regulatorischen Anforderungen konsequent in die eigenen Strukturen integriert werden.

3.3 NIS2-Richtlinie

Mit der NIS2-Richtlinie aus dem Jahr 2023 etabliert die EU einen harmonisierten Sicherheitsrahmen, der das Schutzniveau digitaler Dienste und kritischer Infrastrukturen deutlich anhebt. Die Richtlinie weitet den Anwendungsbereich erheblich aus: Neben klassischen Sektoren wie Energie, Wasser, Gesundheit, Verkehr und digitaler Infrastruktur werden nun u. a. IT-Dienstleister, Cloud-Anbieter sowie öffentliche Verwaltung auf zentraler und regionaler Ebene erfasst. Die Richtlinie gilt grundsätzlich für mittlere und große Einrichtungen dieser Sektoren. Nachdem das NIS2-

[3] Orientierungshilfe zum datenschutzkonformen Einsatz von KI im öffentlich-rechtlichen Rundfunk – Rundfunkdatenschutz

Umsetzungs- und Cybersicherheitsgesetz (NIS2UmsuCG) in Deutschland am 6. Dezember 2025 in Kraft getreten ist, entfalten die Regelungen der NIS2-Richtlinie seitdem ihre Wirkung für die benannten Sektoren sowie für die Verwaltung auf Bundesebene.

Die Rundfunkanstalten werden in den NIS2-Sektoren nicht ausdrücklich genannt. Weder die Liste der „wesentlichen“ noch der „wichtigen“ Einrichtungen umfasst Medien- oder Rundfunkunternehmen. Die Richtlinie adressiert vielmehr digitale Infrastrukturen (z. B. Cloud-Dienste, Online-Marktplätze, Suchmaschinen) sowie klassische Kritische Infrastrukturen. Damit fallen Rundfunkanstalten grundsätzlich nicht automatisch in den Anwendungsbereich der NIS2-Richtlinie, solange sie nicht selbst als Betreiber einer der definierten kritischen oder digitalen Infrastrukturen auftreten – etwa durch den eigenständigen Betrieb von Cloud-Diensten, Content-Delivery-Netzwerken oder Plattformdiensten, die als digitale Dienste im Sinne der Richtlinie einzustufen wären.

Unabhängig davon entfaltet NIS2 erhebliche Wirkung für Datenschutz und Datensicherheit: Die Richtlinie verpflichtet betroffene Einrichtungen zur strukturierten Identifikation, Bewertung und Reduktion von Cybersicherheitsrisiken. Dazu gehören Maßnahmen wie Netzwerksicherheit, Zugriffskontrollen, Backup-Strategien, Verschlüsselung und Anomalie-Monitoring. Besonders relevant sind eng geregelte Meldefristen bei Sicherheitsvorfällen sowie die Pflicht, Lieferkettenrisiken systematisch zu bewerten. Diese Vorgaben wirken direkt auf Art. 32 DSGVO ein und erhöhen ab 2025 spürbar die Anforderungen an die Sicherheit der Verarbeitung.

Auch wenn Rundfunkanstalten formal nicht zum Pflichtenkreis der NIS2 gehören, werden sie die Entwicklungen faktisch berücksichtigen müssen: Zum einen, weil viele ihrer Dienstleister (z. B. Cloud- oder IT-Infrastrukturprovider) unmittelbar NIS2-pflichtig werden und daraus erhöhte Anforderungen entlang der Lieferkette entstehen. Zum anderen, weil der Standard technischer und organisatorischer Maßnahmen im Sinne der DSGVO durch NIS2 de facto angehoben wird. Für die Rundfunkanstalten ergibt sich damit ein wachsender Handlungsdruck, Sicherheitsstandards, Incident-Response-Strukturen und Lieferkettenkontrollen mindestens an das Niveau der NIS2-Pflichten anzulehnen, auch wenn keine unmittelbare rechtliche Verpflichtung besteht.

3.4 Einwilligungsverwaltungsverordnung (EinwV)

Seit dem 1. April 2025 gilt die Einwilligungsverwaltungsverordnung (EinwV) als zentrale Ausführungsregel des TDDDG. Sie schafft die Grundlage für anerkannte Dienste zur Einwilligungsverwaltung, über die Nutzerinnen und Nutzer ihre Einwilligungen nach § 25 TDDDG

zentral und dauerhaft verwalten können. Diese Dienste müssen zuvor von der BfDI[4] anerkannt werden und strenge Anforderungen an Sicherheit, Nutzerfreundlichkeit und Interoperabilität erfüllen.

Für Anbieter digitaler Dienste – und damit auch für Rundfunkanstalten mit entsprechenden Online-Angeboten – bedeutet dies, dass sie die Entscheidungen der Nutzerinnen und Nutzer künftig verbindlich berücksichtigen und technisch verlässlich einbinden müssen (§§ 18–20 EinwV). Die Nutzung eines anerkannten Einwilligungsverwaltungsdienstes durch die Anbieter bleibt zwar freiwillig, entfaltet aber unmittelbare Wirkung, sobald sich Nutzerinnen und Nutzer für einen solchen Dienst entscheiden.

Damit markiert die EinwV einen wichtigen Schritt hin zu klareren, weniger manipulationsanfälligen und datenschutzfreundlicheren Einwilligungsprozessen. Die Verordnung soll innerhalb von zwei Jahren evaluiert werden, um ihre Wirksamkeit zu überprüfen und den Weg für eine europaweit einheitliche Lösung zu ebnen.

Am Rande sei erwähnt, dass ein Anbieter eines zwischenzeitlich anerkannten Dienstes zur Einwilligungsverwaltung im Berichtsjahr mit der Aufsichtsbehörde sowie auch mit den Rundfunkanstalten in Kontakt trat, um den Dienst sowie die Auswirkungen auf den Datenschutz unverbindlich vorzustellen. Als Aufsichtsbehörde begrüße ich grundsätzlich solche Dienste zur Einwilligungsverwaltung, wenn diese tatsächlich die Chance bieten, Einwilligungsprozesse verständlicher und datenschutzfreundlicher zu machen. Diesen Eindruck konnte ich exemplarisch gewinnen.

Gleichwohl müssen die Rundfunkanstalten und Beteiligungsunternehmen im Rahmen ihrer Verantwortlichkeit selbst prüfen, inwieweit sie die Nutzung derartiger Dienste beispielsweise durch eigene Hinweise auf die Möglichkeit der Einwilligungserteilung durch einen anerkannten Dienst zur Einwilligungsverwaltung befördern möchten. Die Aufsichtsbehörde sieht von Empfehlungen ab, da auch die bisherige Einwilligungspraxis über Cookies grundsätzlich den gesetzlichen Anforderungen entspricht.

3.5 Digitaler Omnibus – geplante Änderungen DSGVO

Im November 2025 hat die Europäische Kommission angekündigt, zentrale digitale Rechtsakte – darunter die EU-Datenschutz-Grundverordnung (DSGVO), die KI-Verordnung sowie flankierende Regelwerke – zu überarbeiten und in einem sogenannten Digitalen Omnibus zusammenzuführen.

[4] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Ziel ist eine Vereinfachung und Kostenreduktion bei der Einhaltung rechtlicher Vorgaben sowie die Stärkung der Wettbewerbsfähigkeit im europäischen Binnenmarkt. Der Kommissionsvorschlag beschreibt das Vorhaben selbst als „Soforthilfe“ für Unternehmen, Behörden und Bürgerinnen und Bürger, indem technische Anpassungen an bestehendem Digitalrecht vorgenommen werden, ohne fundamentale Schutzziele aufzugeben.

Nach aktuellem Vorschlag[5] soll auch die DSGVO teilweise novelliert werden. Kern des Vorhabens ist eine erleichterte Datennutzung, insbesondere für KI-gestützte Verarbeitung. Es ist zu befürchten, dass das bestehende Datenschutzniveau damit sinken könnte, da Kontroll- und Transparenzrechte der Betroffenen eingeschränkt werden und bestimmte Schutzmechanismen abgeschwächt werden könnten. Dies betrifft insbesondere die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO). Nach dem Vorschlag sollen sensible Daten künftig für die Entwicklung und den Betrieb von KI-Systemen sowie für biometrische Identitätskontrollen verarbeitet werden dürfen, sofern bestimmte technische Schutzmaßnahmen eingehalten werden.

Auch die Betroffenenrechte sollen eingeschränkt werden. Der neue Art. 12 Abs. 5 DSGVO soll es ermöglichen, Anträge – insbesondere Auskunftsbegehren – abzulehnen oder nur gegen Entgelt zu beantworten, wenn diese „zu anderen Zwecken als dem Schutz der eigenen Daten“ gestellt werden. Der Vorschlag kehrt sich damit von der bisherigen EuGH-Rechtsprechung ab, die ausdrücklich bestätigte, dass Betroffene mit dem Auskunftsrecht auch sachfremde Ziele verfolgen dürfen. Zudem soll das Beweismaß für „exzessive“ Anträge reduziert werden, was es Verantwortlichen erleichtern dürfte, Anträge als missbräuchlich einzustufen.

Bei den Informationspflichten (Art. 13 DSGVO) sind ebenfalls Erleichterungen vorgesehen: Verantwortliche sollen unter bestimmten Umständen von der Informationspflicht entbunden werden, etwa wenn personenbezogene Daten im Rahmen klar umgrenzter, nicht datenintensiver Beziehungen erhoben wurden (z. B. Beschäftigung, Vereinsmitgliedschaft). Dies soll Bürokratie abbauen, birgt aber zugleich Risiken für die Transparenz gegenüber Betroffenen.

Besonders weitreichend ist die geplante Änderung zu KI-Bezug und berechtigtem Interesse (neuer Art. 88c DSGVO). Danach sollen die Entwicklung und der Betrieb von KI-Systemen grundsätzlich als „berechtigtes Interesse“ gelten. Problematisch ist, dass sensible Daten (Art. 9 DSGVO) hierfür künftig ohne Einwilligung nutzbar wären, während „normale“ Daten (für andere Verarbeitungen) weiterhin einer Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO) unterliegen würden. Wenn die Rechtsgrundlage des berechtigten Interesses in Art. 88c DSGVO bei der Entwicklung und dem Betrieb von KI-Systemen bereits ohne Abwägung angenommen wird, stellt das einen Wertungswiderspruch dar, der den Kern des bisherigen Schutzkonzepts der DSGVO an dieser Stelle

[5] Vorschlag vom 19.11.2025: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837

massiv aushebelt. Durch die Regelung wird das bisherige Schutzkonzept umgekehrt, wonach sensible Daten bisher am strengsten geschützt werden. Eine solche Pauschalisierung der Rechtsgrundlage des berechtigten Interesses - auch aus politischem Innovationsdruck - ist äußerst kritisch zu sehen, da damit eine Entkopplung von Risiko und Schutz erfolgt, dies vor dem Hintergrund der grundrechtlichen Basis der DSGVO als Regelungsregime zum Schutz der informationellen Selbstbestimmung. Auch der technologieneutralen Konzeption der DSGVO wird damit widersprochen.

Relevant sind ebenso die Regelungen zur Verarbeitung in Endeinrichtungen in Art. 88a/b DSGVO. Damit wird eine EU-weit einheitliche Einwilligungspflicht für Zugriffe auf Endgeräte eingeführt – mit Ausnahmen für sicherheitsrelevante oder nutzerinitiierte Vorgänge. Mediendienste-Anbieter sollen ausdrücklich privilegiert werden, um den Schutz des Medienpluralismus zu gewährleisten. Es soll einen neuen Katalog von Fällen geben, in denen die Verwendung von Cookies (und ähnlichen Technologien) auch ohne Einwilligung zulässig ist (z. B. für Reichweitenmessung). Darüber hinaus soll das Einwilligungsmanagement angepasst werden: Browser oder Betriebssysteme sollen künftig standardisiert an Webseiten übermitteln können, ob Nutzer Cookies (oder ähnliche Technologien) grundsätzlich akzeptieren oder ablehnen. Damit wird der bisherige Vorrang der ePrivacy-Richtlinie (RL 2002/58) und des deutschen TDDDG bei Endgerätezugriffen zu einem Vorrang in Richtung DSGVO verschoben. Die EinwV (siehe Kapitel 3.4), die ein Instrument zur technischen Umsetzung von Einwilligungen ist, ist davon jedoch nicht betroffen, da Art. 88a DSGVO lediglich festlegt, wofür eine Einwilligung zwingend erforderlich sein soll.

Weitere relevante Änderungskomplexe betreffen:

- **Pseudonymisierung (Art. 41a DSGVO)**: Die Kommission soll mittels Durchführungsrechtsakten Kriterien dafür festlegen, wann pseudonymisierte Daten für bestimmte Empfänger faktisch nicht mehr personenbezogen sind. Dieser Vorschlag ist angesichts der jüngsten EuGH-Rechtsprechung sehr umstritten (siehe dazu Kapitel 3.6.1).
- **Meldepflichten bei Datenschutzverletzungen (Art. 33 DSGVO)**: Künftig sollen nur noch Datenpannen mit hohem Risiko meldepflichtig sein; Meldungen erfolgen nicht mehr bei den Aufsichtsbehörden, sondern über eine zentrale EU-Anlaufstelle unter Leitung der ENISA[6]. Soweit damit eine Vereinfachung der Meldepflichten erfolgen soll, könnte auch mit dieser Änderung ein sinkendes Datenschutzniveau einhergehen. Ob sich die geplante Kompetenzverschiebung für die Effektivität der Meldewege wirklich bezahlt macht, kann zumindest angezweifelt werden.

Wie diese Änderungen sich tatsächlich auswirken, hängt zunächst davon ab, wie stark die genannten bemerkenswerten Anpassungen der Regelwerke wirklich ausfallen. Es gilt somit das weitere

[6] Agentur der Europäischen Union für Cybersicherheit (European Network and Information Security Agency)

Gesetzgebungsverfahren abzuwarten; Rat und Parlament befinden sich seit Ende 2025 in der ersten Lesung.

3.6 EDSA-Stellungnahmen und Leitlinien

Der Europäische Datenschutzausschuss (EDSA), auf EU-Ebene als European Data Protection Board (EDPB) bezeichnet, hat die Aufgabe, eine einheitliche Auslegung und Anwendung der Datenschutz-Grundverordnung sicherzustellen. Er veröffentlicht hierzu Leitlinien und Stellungnahmen, die sowohl von den deutschen Aufsichtsbehörden als auch in meiner eigenen Aufsichtspraxis herangezogen werden.

Nachfolgend berichte ich über ausgewählte Veröffentlichungen mit Relevanz für die Verantwortlichen und auch für meine Aufsichtstätigkeit.

3.6.1 Leitlinien zur Pseudonymisierung

Der Europäische Datenschutzausschuss (EDSA) hat im Januar 2025 neue Leitlinien zur Pseudonymisierung veröffentlicht, die sowohl rechtliche als auch technische Anforderungen an eine wirksame Pseudonymisierung konkretisieren. Die Leitlinien betonen, dass pseudonymisierte Daten weiterhin personenbezogene Daten bleiben, solange sie mithilfe zusätzlicher Informationen einer Person zugeordnet werden können, und daher vollständig den Vorgaben der DSGVO unterliegen. Zugleich hebt der EDSA hervor, dass Pseudonymisierung maßgeblich zur Risikoreduktion beitragen und insbesondere die Nutzung berechtigter Interessen als Rechtsgrundlage sowie die Bewertung der Zweckkompatibilität unterstützen kann. Zudem zeigt der Ausschuss, wie Pseudonymisierung zentrale Datenschutzpflichten wie die Umsetzung der Datenschutzgrundsätze, „Privacy by Design“ und geeignete Sicherheitsmaßnahmen fördert.

In technischer Hinsicht beschreiben die Leitlinien verschiedene Transformationsverfahren zur Entfernung oder Ersetzung identifizierender Merkmale sowie die zwingend getrennte Aufbewahrung der für eine Re-Identifizierung erforderlichen Zusatzinformationen. Dazu zählen etwa kryptografische Verfahren oder Zuordnungstabellen, deren Schutz ein zentrales Element wirksamer Pseudonymisierung darstellt. Ergänzend enthalten die Leitlinien praktische Beispiele, die die Anwendung in unterschiedlichen Verarbeitungsszenarien illustrieren, etwa zur Datenminimierung, zur Sicherstellung von Zweckbindung und Vertraulichkeit oder zur risikobasierten Bewertung weiterer Verarbeitungsschritte.

Für Rundfunkanstalten sind die Leitlinien insbesondere insofern relevant, als sie eine klarere Orientierung für datenschutzkonforme Datenverarbeitungsprozesse geben, etwa bei Analysen von

Nutzungsdaten. Darüber hinaus erleichtert die präzisierte Rolle der Pseudonymisierung die risikobasierte Ausgestaltung digitaler Dienste und unterstützt bei Kooperationen mit externen Partnern, insbesondere wenn Datentransfers mit erhöhtem Schutzbedarf verbunden sind.

3.6.2 Leitlinien zum Zusammenspiel von DSA und DSGVO

Der Europäische Datenschutzausschuss (EDSA) hat im September 2025 Leitlinien zum Zusammenspiel zwischen dem Digital Services Act (DSA)[7] und der DSGVO veröffentlicht, um eine kohärente Anwendung beider Regelwerke sicherzustellen. Sie betreffen insbesondere DSA-Pflichten, die auf DSGVO-Begriffe wie Profiling oder besondere Kategorien personenbezogener Daten zurückgreifen, und daher datenschutzrechtliche Anforderungen auslösen.

Die Leitlinie hebt hervor, dass zentrale DSA-Vorgaben – etwa Melde- und Beschwerdeverfahren, Empfehlungssysteme, Werbetransparenz sowie der Schutz Minderjähriger – datenschutzkonform umzusetzen sind und sich strikt an den Grundsätzen der DSGVO orientieren müssen. Zudem erläutert sie, wie Plattformen personenbezogene Daten im Rahmen von Prüfungen illegaler Inhalte oder automatisierten Prozessen rechtmäßig verarbeiten und welche Grenzen für Profiling und datenbasierte Werbung gelten.

Ein weiterer Schwerpunkt liegt auf der künftigen Zusammenarbeit zwischen Datenschutzbehörden und den für den DSA zuständigen Stellen, um eine abgestimmte und wirksame Aufsicht über beide Regelwerke sicherzustellen. Insgesamt trägt die Leitlinie dazu bei, eine einheitliche datenschutzrechtliche Bewertung DSA-bezogener Verarbeitungstätigkeiten zu ermöglichen und die Rechtssicherheit für Plattformen, Behörden und betroffene Personen zu erhöhen.

3.6.3 Gemeinsame Leitlinie von EDSA und Europäischer Kommission zu DMA und DSGVO

Der Europäische Datenschutzausschuss (EDSA) und die Europäische Kommission haben im Oktober 2025 erstmals gemeinsame Leitlinien zum Zusammenspiel von Digital Markets Act (DMA)[8] und DSGVO veröffentlicht. Sie sollen sicherstellen, dass Gatekeeper-Plattformen DMA-Pflichten – etwa zur Kombination oder bereichsübergreifenden Nutzung personenbezogener Daten – nur unter strikt datenschutzkonformen Bedingungen umsetzen, insbesondere im Hinblick auf Wahlmöglichkeiten und wirksame Einwilligungen nach Art. 5 Abs. 2 DMA.

Für die Datenschutzaufsicht bedeutet dies, dass künftig besonders zu prüfen ist, ob Gatekeeper ihre Marktverhaltenspflichten im Einklang mit den DSGVO-Grundsätzen erfüllen. Die Leitlinie stärkt

[7] Zu Inhalt und Bedeutung des DSA für die Rundfunkanstalten siehe Tätigkeitsbericht 2023, Kapitel 3.1.1
[8] Zu Inhalt und Bedeutung des DMA für die Rundfunkanstalten siehe Tätigkeitsbericht 2023, Kapitel 3.1.2

zudem die koordinierte Zusammenarbeit zwischen Datenschutzbehörden und den für den DMA zuständigen Stellen.

Für Rundfunkanstalten ist die Leitlinie vor allem insoweit relevant, als sie häufig Dienste großer Gatekeeper nutzen und daher von deren datenschutz- und DMA-konformer Datenverarbeitung – etwa bei Datenzugang, Interoperabilität oder Plattformfunktionen – mittelbar betroffen sind.

3.7 Rechtsprechung

Es bleibt unerlässlich, die aktuelle datenschutzrechtliche Rechtsprechung – insbesondere auf europäischer Ebene – fortlaufend zu verfolgen. Dieses Kapitel soll einen Überblick über ausgewählte relevante Entscheidungen aus der Rechtsprechung geben, die Einfluss auf die Arbeit der Aufsichtsbehörde sowie auf die beaufsichtigten Rundfunkanstalten und deren Beteiligungsunternehmen haben können.

3.7.1 Negative Gefühle als immaterieller Schaden – Voraussetzung des Kontrollverlustes

Die Gerichte befassten sich in der Vergangenheit immer wieder mit der Frage, welche Voraussetzungen vorliegen müssen, um einen immateriellen Schaden im Sinne des Art. 82 DSGVO zu begründen.

Auf eine Vorlage des Bundesgerichtshofs vom 26. September 2023 (VI ZR 97/22) hat der Europäische Gerichtshof mit Urteil vom 4. September 2025 (C-655/23) nun wichtige Klarstellungen zum Verständnis des immateriellen Schadens gemäß Art. 82 DSGVO getroffen. Der EuGH stellte fest, dass der Begriff des immateriellen Schadens auch negative Gefühle umfassen kann, die eine betroffene Person infolge einer unbefugten Übermittlung ihrer personenbezogenen Daten an einen Dritten empfindet. Dazu zählen insbesondere Sorge, Ärger oder ähnliche emotionale Belastungen, die durch einen Verlust der Kontrolle über die Daten, die Möglichkeit ihrer missbräuchlichen Verwendung oder eine mögliche Rufschädigung hervorgerufen werden. Voraussetzung für einen Anspruch ist jedoch, dass die betroffene Person nachweist, dass sie tatsächlich solche Gefühle und deren negative Folgen aufgrund des jeweiligen Datenschutzverstoßes erlebt hat. Bloße abstrakte Befürchtungen oder theoretische Risiken genügen nicht.

Dem Urteil lag ein Bewerbungsverfahren zugrunde, in dessen Rahmen eine Bank Bewerberdaten irrtümlich an einen unbeteiligten Dritten weitergeleitet hatte. Die unterschiedlichen Bewertungen der Vorinstanzen führten schließlich zur Vorlage an den EuGH, der nun den unionsrechtlichen Rahmen für immaterielle Schadensersatzansprüche weiter präzisiert hat. Dessen ungeachtet bleibt

spannend, wie in Zukunft betroffene Personen die „negativen Gefühle“ über den Kontrollverlust nachweisen.

Die Frage des erforderlichen Kontrollverlustes beschäftigte im Berichtsjahr aber auch nationale Gerichte: Der Bundesgerichtshof hat mit Urteil vom 11. November 2025 (VI ZR 396/24) hervorgehoben, dass bereits der Kontrollverlust über personenbezogene Daten als solcher einen immateriellen Schaden im Sinne des Art. 82 Abs. 1 DSGVO darstellen kann, selbst wenn die Daten bereits zuvor kompromittiert worden waren. Maßgeblich sei, dass der Verantwortliche seine Pflichten – insbesondere im Zusammenhang mit der Beendigung eines Auftragsverarbeitungsverhältnisses – verletzt habe und dadurch ein zusätzlicher unbefugter Zugriff ermöglicht wurde. Verbleiben Daten nach Auftragsende beim Auftragsverarbeiter und werden dort abgegriffen, liegt nach Auffassung des BGH ein ersatzfähiger Schaden vor, da die betroffene Person erneut und vertieft die Kontrolle über ihre Daten verliert. Der BGH betonte dabei ausdrücklich die Pflicht des Verantwortlichen, nachweisbar sicherzustellen, dass personenbezogene Daten beim Auftragsverarbeiter tatsächlich gelöscht oder zurückgegeben wurden. Ein bloßes Vertrauen auf angekündigte Löschungen genüge nicht.

Eine andere Akzentuierung nahm das OLG Saarbrücken in seinem Urteil vom 17. Dezember 2025 (5 U 65/24) vor. Es verneinte einen immateriellen Schaden wegen Kontrollverlustes, wenn ein Anspruchsteller die Kontrolle über seine Daten bereits vor dem schädigenden Ereignis durch eigenes Verhalten aufgegeben hatte. Im entschiedenen Fall stammten die betroffenen personenbezogenen Daten aus einem Scraping-Vorfall, der über fünf Jahre zurücklag. Das Gericht stellte fest, dass ein Schaden ausscheidet, wenn der Betroffene die Daten zuvor selbst in einer Weise veröffentlicht hat, die mit einem Risiko unkontrollierter Weiterverbreitung verbunden war. Ebenso lehnte das OLG einen Unterlassungsanspruch ab, wenn der Betroffene durch eigene Einstellungen (z. B. in sozialen Netzwerken) die weitere Verarbeitung selbst hätte verhindern können.

Die Entscheidungen zeigen deutlich, dass der „Kontrollverlust“ als zentrales Kriterium für immaterielle Schäden zunehmend konturiert wird: Während EuGH und BGH den Kontrollverlust bereits als eigenständigen Schaden anerkennen – sofern er auf einen objektiv feststellbaren Datenschutzverstoß zurückgeht – betont das OLG Saarbrücken die Eigenverantwortung der betroffenen Person. Für die Rundfunkanstalten bedeutet dies, dass sowohl die Sicherstellung wirksamer Löschprozesse als auch die Dokumentation datenschutzkonformer Abläufe weiter an Bedeutung gewinnen; gleichzeitig verdeutlichen die Entscheidungen die Notwendigkeit, Betroffene transparent über eigene Mitverantwortlichkeiten und Einstellungsmöglichkeiten zu informieren.

3.7.2 Klage auf Nichtigerklärung des EU-Angemessenheitsbeschlusses (Urteil des EuG)

Mit Urteil vom 3. September 2025 hat das Gericht der Europäischen Union (EuG) die Nichtigkeitsklage des französischen Abgeordneten Philippe Latombe gegen den Angemessenheitsbeschluss zum EU-US Data Privacy Framework (DPF) abgewiesen und bestätigt, dass die USA zum Zeitpunkt des Beschlusses im Jahr 2023 ein angemessenes Datenschutzniveau gewährleisteten. Das Gericht sah insbesondere den neu geschaffenen Data Protection Review Court (DPRC), der durch die Executive Order 14086 im Jahr 2022 eingerichtet wurde, als institutionell ausreichend unabhängig an. Das Gremium soll es den europäischen Bürgern ermöglichen, Beschwerden, die sich mit dem Zugriff US-amerikanischer Nachrichtendienste auf ihre personenbezogenen Daten befassen, prüfen zu lassen.

Gegen das Urteil wurde allerdings Rechtsmittel eingelegt; das Verfahren ist nun unter dem Aktenzeichen C-703/25 P beim Europäischen Gerichtshof anhängig. Damit wird der EuGH – wie bereits in „Schrems I“ und „Schrems II“ – erneut die Rechtmäßigkeit eines transatlantischen Datentransferrahmens prüfen. Ob der DPF-Beschluss sowohl formal anfechtbar als auch materiell mit der Grundrechte- und DSGVO-Rechtsprechung vereinbar ist, bleibt somit offen.

Das Urteil bietet daher nur vorläufige Planungssicherheit, aber keine endgültige Stabilität. Zu kritisieren ist weiterhin die starke Abhängigkeit des DPF von präsidialen Executive Orders sowie die weitreichenden Befugnisse der US-Geheimdienste. Sollte das anhängige Verfahren neue Beweisgrundlagen oder breitere Angriffsargumente hervorbringen, ist eine Neubewertung durch den EuGH nicht ausgeschlossen. Der EU-US-Datentransfer bleibt daher ein Dauerbrenner im Datenschutzrecht.

Für Rundfunkanstalten bedeutet das Urteil zunächst, dass Datentransfers in die USA – etwa beim Einsatz von Cloud-Infrastrukturen, Kommunikations- und Analyse-Tools oder Produktionssoftware – weiterhin auf Grundlage des DPF erfolgen können. Angesichts des laufenden Verfahrens vor dem EuGH und der anhaltenden Kritik an der US-Rechtsarchitektur bleibt jedoch ungewiss, ob der Angemessenheitsbeschluss langfristig Bestand haben wird. Die Rundfunkanstalten sollten daher ihre US-bezogenen Datenströme weiterhin regelmäßig prüfen, vertragliche Absicherungen stärken, Alternativen innerhalb der EU erwägen und auf mögliche erneute Veränderungen der Rechtslage vorbereitet bleiben (siehe dazu auch die Empfehlungen der RDSK, Kapitel 9.2.2).

3.7.3 EuGH präzisiert Begriff der personenbezogenen Daten

Der Europäische Gerichtshof hat mit Urteil vom 4. September 2025 (C-413/23 P) wesentliche Fragen zur Anonymität und Personenbeziehbarkeit pseudonymisierter Daten präzisiert. Nach der

Entscheidung ist die Einordnung eines Datums als personenbezogen oder anonym stets aus der Perspektive des jeweils Verantwortlichen zum Zeitpunkt der Erhebung vorzunehmen. Die gleichen Daten können somit für unterschiedliche Verantwortliche einen unterschiedlichen Charakter haben; sie können beim Empfänger anonym sein, obwohl sie beim übermittelnden Verantwortlichen personenbezogen bleiben. Entscheidend ist, ob der Empfänger unter Einsatz vernünftigerweise verfügbarer Mittel eine Identifizierung der betroffenen Person vornehmen kann. Damit bestätigt der EuGH, dass pseudonymisierte Daten nicht automatisch für alle Empfänger personenbezogen sind, sondern im konkreten Kontext anonym sein können, sofern keine Re-Identifizierungsmöglichkeit besteht.

Das Urteil erleichtert künftig die Annahme von anonymen Daten dort, wo beim Empfänger keine Identifizierbarkeit besteht. Dies hat insbesondere für die Rundfunkanstalten Auswirkungen auf die Rechtmäßigkeit des Einsatzes von Tools zur Nutzungsmessung (siehe dazu auch Kapitel 3.1 und ebenso 3.5 des Tätigkeitsberichts 2024 zu Anpassungen durch den Reformstaatsvertrag für Leistungsanalysen, sowie Kapitel 6.1 im Tätigkeitsbericht 2024).

Auch der EU-Gesetzgeber hat mit dem aktuellen Gesetzgebungsprozess zum Digitalen Omnibus (siehe Kapitel 3.5) Änderungsvorschläge zur DSGVO vorgelegt, die sich jedoch von den Standpunkten des EuGH-Urteils unterscheiden. Während der EuGH eine kontext- und empfängerbezogene Prüfung zur Feststellung der Personenbezogenheit des Datums vorsieht und damit die DSGVO-Dogmatik bestätigt, unterschreitet der Regelungsentwurf aus dem Digitalen Omnibus das vom EuGH vorgegebene Schutzniveau, indem er den Personenbezug als Folge einer Identifizierbarkeitsprüfung im Einzelfall exekutiv festlegen will. Der Prüfmaßstab wird durch die Omnibus-Regelung in der Weise verengt, dass Informationen nicht allein deshalb personenbezogen werden sollen, weil ein möglicher anderer Empfänger eine Identifizierung vornehmen könnte.

Zur Veranschaulichung ein einfaches Beispiel:

Das Unternehmen A erhebt Daten und kennt die Identität der Person, auf die sich die Daten beziehen. Das Unternehmen B verarbeitet die Daten in pseudonymisierter Form weiter. Eine Re-Identifikation dieser pseudonymisierten Daten ist gemeinsam möglich. Folgt man der EuGH-Rechtsprechung bliebe damit der Personenbezug bestehen (systemische Betrachtung), die Pseudonymisierung wäre nicht als relative Anonymisierung einzustufen. Folgt man dem Digitalen Omnibus, sind die Daten bei B ggf. nicht personenbezogen, da es auf andere Empfänger nicht ankommt, sodass die DSGVO-Pflichten dort entfallen könnten.

Während nach dem EuGH der Personenbezug dem realen Macht- und Wissensgefüge folgt, folgt nach dem Digitalen Omnibus der Personenbezug der formalen Position eines einzelnen Akteurs.

Hier wird sehr genau hinzuschauen sein, ob und inwieweit der EU-Gesetzgeber den bisherigen Entwurf des Digitalen Omnibus noch entsprechend der Auslegung des EuGH anpasst.

3.7.4 Facebook-Fanpages

Mit Bescheid vom 17. Februar 2023 untersagte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) dem Bundespresseamt (BPA) den Betrieb seiner Facebook-Fanpage, da ein datenschutzkonformer Betrieb nach Auffassung der Aufsicht nicht möglich sei. Grundlage war unter anderem die Entscheidung des EuGH vom 5. Juni 2018 (C-210/16), wonach Betreiber einer Facebook-Fanpage datenschutzrechtlich mitverantwortlich sind. Gegen die Untersagung erhob das BPA Klage. Das Verwaltungsgericht Köln hob mit Urteil vom 17. Juli 2025 (Az. 13 K 1419/23) die Verfügung auf und stellte fest, dass nicht das BPA, sondern allein Meta, als die Betreiberin von Facebook, zur Einholung wirksamer Einwilligungen für den Einsatz von Cookies verpflichtet ist. Zwischen dem Betrieb der Fanpage und dem Setzen oder Auslesen der Cookies bestehe kein zurechenbarer Zusammenhang, da diese bei jedem Besuch einer Facebook-Seite platziert werden können. Das BPA darf seine Fanpage daher vorerst weiterbetreiben.

Allerdings ist die Entscheidung nicht rechtskräftig, die BfDI hat Berufung eingelegt. Sie verwies dabei auf die bestehende Rechtsunsicherheit für Bundesbehörden bei der Nutzung sozialer Netzwerke und veröffentlichte parallel eine Handreichung, die notwendige Schritte für eine rechtssichere Nutzung darstellt. Zugleich betonte sie, dass verbindliche Rahmenbedingungen entweder durch den Gesetzgeber oder eine letztinstanzliche Entscheidung geschaffen werden müssten.

Die Entwicklung in diesem Verfahren verfolge ich weiter aufmerksam, da sie Rückschlüsse auf die Anforderungen an den datenschutzkonformen Betrieb von Social-Media-Angeboten auch für den öffentlich-rechtlichen Rundfunk zulässt.

3.7.5 Datenschutzrechtliche Verantwortlichkeit von Arbeitnehmern

Der Bundesgerichtshof hat mit Beschluss vom 7. Oktober 2025 (VI ZR 297/24) bekräftigt, dass Arbeitnehmer grundsätzlich keine Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO sind. Sie handeln im Regelfall weisungsgebunden und damit als dem Verantwortlichen „unterstellte Personen“ im Sinne von Art. 29 DSGVO. Eine eigene datenschutzrechtliche Verantwortlichkeit kommt erst in Ausnahmefällen in Betracht, etwa wenn Beschäftigte bewusst und eigenständig entgegen internen Vorgaben handeln und damit selbst über Zwecke und Mittel der Verarbeitung entscheiden („Mitarbeiterexzess“ – siehe dazu auch Kapitel 6.11).

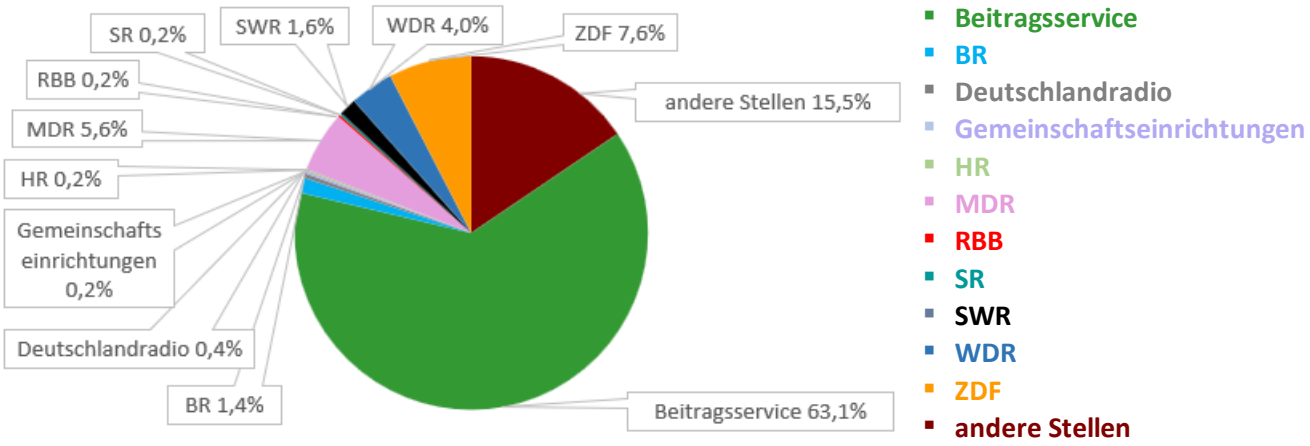
Der BGH verweist dabei auf die Rechtsprechung des EuGH, wonach Arbeitnehmer im Normalfall nicht selbstbestimmt handeln, sondern organisatorisch in die Struktur des Verantwortlichen eingebunden sind. Damit liegt die datenschutzrechtliche Verantwortung regelmäßig bei der Organisation bzw. dem Arbeitgeber, der über Zwecke und Mittel der Verarbeitung entscheidet und die Einhaltung der DSGVO sicherstellen muss. Für Betroffene bedeutet dies, dass Ansprüche grundsätzlich gegenüber der verantwortlichen Stelle und nicht gegenüber einzelnen Beschäftigten geltend zu machen sind.

Die Entscheidung stärkt die Rechtssicherheit im Beschäftigtendatenschutz und bestätigt, dass Compliance- und Haftungsverantwortung organisatorisch zu verorten sind. Zugleich bleibt die Möglichkeit bestehen, einzelne Beschäftigte in Fällen eigenmächtigen, zweckwidrigen Handelns als Verantwortliche heranzuziehen.

4 Eingaben beim Rundfunkdatenschutzbeauftragten

Der Rundfunkdatenschutzbeauftragte ist zuständig für die Bearbeitung von Beschwerden. In § 31l Abs. 5 MStV ist nunmehr das Beschwerderecht zentral geregelt. Mit dieser Regelung des Reformstaatsvertrages bedarf es seit 2026 keines Rückgriffs auf die Regelungen der einzelnen Bundesländer mehr. Gemäß § 31l Abs. 5 MStV kann sich jeder unmittelbar an den Rundfunkdatenschutzbeauftragten wenden, um eine Verletzung seiner Rechte vorzutragen. Im Übrigen wird das Recht auf Beschwerde bei einer Aufsichtsbehörde durch Art. 77 DSGVO gewährleistet.

Im Jahr 2025 erreichten die Aufsichtsbehörde 502 Eingaben:



Eingaben gesamt	Anzahl	Prozent
Beitragsservice	**317**	63,1%
Beteiligungsunternehmen	**0**	0,0%
BR	**7**	1,4%
Deutschlandradio	**2**	0,4%
Gemeinschaftseinrichtungen	**1**	0,2%
HR	**1**	0,2%
MDR	**28**	5,6%
RBB	**1**	0,2%
SR	**1**	0,2%
SWR	**8**	1,6%
WDR	**20**	4,0%
ZDF	**38**	7,6%
andere Stellen	**78**	15,5%
Gesamtergebnis	**502**	**100,0%**

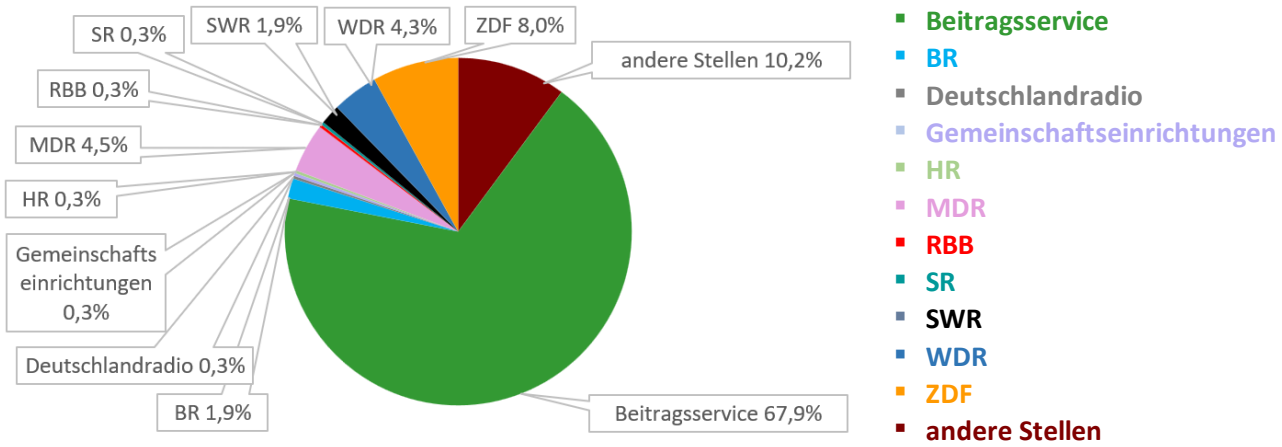
423 der Eingaben (84,3 %) konnten direkt den von uns beaufsichtigten Rundfunkanstalten zugeordnet werden, 78 Eingaben (15,5 %) betrafen andere Einrichtungen/Stellen, die nicht unserer Aufsicht unterliegen, 1 Eingabe (0,2 %) erreichte uns im Hinblick auf Gemeinschaftseinrichtungen.

Die Gesamtzahl der Eingaben unterteilte sich thematisch in:

- 374 Beschwerden (74,5 %) und
- 128 sonstige Eingaben (25,5 %).

4.1 Beschwerden

Die 374 eingegangenen Beschwerden verteilten sich wie folgt auf die Rundfunkanstalten. Unter dem Punkt „andere Stellen“ sind Beschwerden zusammengefasst, die keiner spezifischen Rundfunkanstalt, die unserer Aufsicht unterliegt, zugeordnet werden konnten, so z. B. Beschwerden, die die ARD oder den im Berichtszeitraum noch nicht unserer Zuständigkeit unterfallenden NDR betrafen. 18 Beschwerden mit datenschutzrechtlichem Bezug waren begründet (4,8 %).



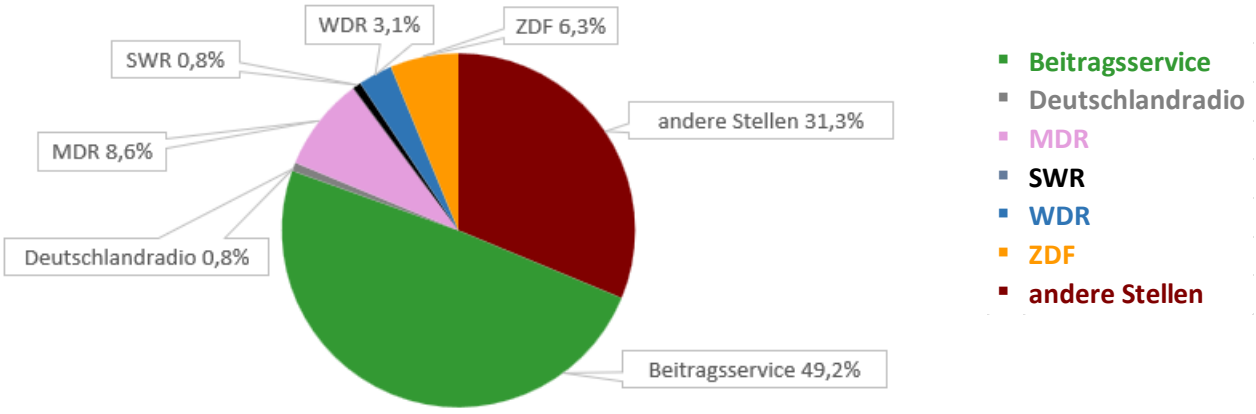
Beschwerden	Anzahl	Prozent	begründet	Prozent
Beitragsservice	**254**	67,9%	13	72,2%
Beteiligungsunternehmen	**0**	0,0%	0	0,0%
BR	**7**	1,9%	1	5,6%
Deutschlandradio	**1**	0,3%	0	0,0%
Gemeinschaftseinrichtungen	**1**	0,3%	0	0,0%
HR	**1**	0,3%	0	0,0%
MDR	**17**	4,5%	0	0,0%
RBB	**1**	0,3%	0	0,0%
SR	**1**	0,3%	0	0,0%
SWR	**7**	1,9%	1	5,6%
WDR	**16**	4,3%	3	16,7%
ZDF	**30**	8,0%	0	0,0%
andere Stellen	**38**	10,2%	0	0,0%
Gesamtergebnis	**374**	**100,0%**	**18**	**100,0%**
davon begründet	**18**	**4,8%**		

4.2 Sonstige Eingaben

Unter die sonstigen Eingaben werden Zuschriften gefasst, die von vermeintlichen Datenschutzthemen und fehlgeleiteten Auskunftsersuchen über Anfragen/Mitteilungen zum Beitragseinzug oder Programm bis hin zur Beratung zu Datenschutzthemen reichen.

Unter den 128 sonstigen Eingaben befanden sich 88 mit direktem Bezug zu einer Rundfunkanstalt (68,7 %). Unter dem Punkt „andere Stellen“ sind 40 Eingaben (31,3 %) zusammengefasst, die keiner Rundfunkanstalt, die unserer Aufsicht unterliegt, zugeordnet werden konnten. Dabei handelt es sich

z. B. um Eingaben bezüglich der ARD, Privatsendern oder in der Zuständigkeit anderer Aufsichtsbehörden.



Sonstige Eingaben	Anzahl	Prozent
Beitragsservice	**63**	49,2%
Beteiligungsunternehmen	**0**	0,0%
BR	**0**	0,0%
Deutschlandradio	**1**	0,8%
Gemeinschaftseinrichtungen	**0**	0,0%
HR	**0**	0,0%
MDR	**11**	8,6%
RBB	**0**	0,0%
SR	**0**	0,0%
SWR	**1**	0,8%
WDR	**4**	3,1%
ZDF	**8**	6,3%
andere Stellen	**40**	31,3%
Gesamtergebnis	**128**	**100,0%**

4.3 Entwicklung der Eingaben 2023 bis 2025

Obwohl das Eingabevolumen im Verhältnis zu 2024 konstant geblieben ist, hat sich die Eingabebearbeitung selbst im Jahr 2025 verändert, hin zu einer arbeitsintensiveren Beschwerdebearbeitung.

Entwicklung Eingabekategorie	2023	2024	2025
Beschwerden	131	307	374
Sonstige Eingaben	165	195	128
Gesamt	**296**	**502**	**502**

Zunehmend gehen bei der Aufsichtsbehörde Beschwerden ein, die erkennbar unter Nutzung KI-gestützter Textgenerierung verfasst wurden (siehe dazu auch Kapitel 8.3). Diese Entwicklung wird dadurch begünstigt, dass die Erstellung von Beschwerdeschreiben – einschließlich umfangreicher rechtlicher Erwägungen und Verweise auf rechtliche Grundlagen – durch den Einsatz von KI erheblich vereinfacht worden ist. Allerdings sind die Aussagen und vor allem die Einschätzungen der Rechtslage oft unvollständig oder schlicht falsch.

Das Gesamtaufkommen der Eingaben stieg im Jahr 2024 aufgrund der Aufnahme weiterer Rundfunkanstalten in die Aufsichtszuständigkeit des Rundfunkdatenschutzbeauftragten an und blieb im Jahr 2025 konstant. Die Verteilung der Eingaben auf die verantwortlichen Stellen veränderte sich im Berichtszeitraum nicht wesentlich.

Entwicklung betreffende Stelle	Anzahl 2023	Anzahl 2024	Anzahl 2025
Beitragsservice	182	317	317
BR	5	6	7
Deutschlandradio	3	3	2
Gemeinschaftseinrichtungen	0	0	1
HR	0	2	1
MDR	14	23	28
RBB	3	3	1
SR	1	0	1
SWR	23	15	8
WDR	20	14	20
ZDF	45	55	38
andere Stellen	0	64	73
Gesamt	**296**	**502**	**502**

Für 2026 ist durch die gestiegene Anzahl zu beaufsichtigender Rundfunkanstalten und Beteiligungsunternehmen, die verstärkte Nutzung von KI und konzertierte Aktionen von Rundfunkbeitragsgegnern mit einem deutlichen Anstieg an Eingaben zu rechnen.

4.4 Klagen und Gerichtsverfahren

Selten kommt es auch vor, dass gegen den Rundfunkdatenschutzbeauftragten verwaltungsgerichtliche Klage erhoben wird. Gemäß Art. 78 DSGVO hat jede natürliche oder juristische Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

Eine Beschwerde kann mit einem förmlichen Bescheid des Rundfunkdatenschutzbeauftragten abgeschlossen werden, in dem sowohl der Sachverhalt als auch die rechtlichen Anknüpfungspunkte eingehend beleuchtet und gewürdigt werden. Im Ergebnis ergeht eine entsprechende rechtliche Entscheidung zu der Beschwerde.

Ist die Beschwerde führende Person mit dem Ergebnis der Entscheidung der Aufsichtsbehörde nicht einverstanden, so steht es ihr offen, vor einem Verwaltungsgericht Klage zu erheben, was im Berichtsjahr dreimal geschehen ist. Die Verfahren sind noch nicht abgeschlossen und werden vor den Verwaltungsgerichten in München, Köln und Berlin geführt. In zwei Fällen geht es um Fragen, die im Zusammenhang mit der Datenverarbeitung beim Beitragsservice stehen, und eine weitere Klage befasst sich mit dem Medienprivileg, insbesondere mit der Reichweite und Grenzen dieses Rechtsinstituts. Wann die Verfahren abgeschlossen sind, lässt sich zum jetzigen Zeitpunkt noch nicht prognostizieren. Ich werde weiter berichten.

4.5 Dienstaufsichtsbeschwerde

Von Zeit zu Zeit kommt es vor, dass Beschwerdeführer mit der Art und Weise des Umgangs meiner Behörde mit ihren Beschwerden so unzufrieden sind, dass sie eine Dienstaufsichtsbeschwerde erheben.

Dienstaufsichtsbeschwerden gehören zu Petitionen im Sinne von Art. 17 Grundgesetz und können jegliches dienstliches Verhalten sowie jede Stelle und jeden Amtsträger betreffen. Die Dienstaufsichtsbeschwerde ist aber kein Rechtsbehelf im prozessrechtlichen Sinne; sie wird angesehen als Maßnahme im öffentlichen Dienstrecht.

Im Berichtsjahr habe ich eine rein beitragsrechtliche Angelegenheit ohne Datenschutzbezug wegen mangelnder Zuständigkeit nicht bearbeitet und auf die streitige Auseinandersetzung zwischen dem Beschwerdeführer und dem Beitragsservice verwiesen. Dies habe ich ausführlich begründet und dargelegt, dass ein datenschutzrechtliches Eingreifen erst dann möglich ist, wenn der

beitragsrechtliche Sachverhalt geklärt ist und ggf. eine Beitragspflicht nicht besteht. Sodann kann geprüft werden, ob die (streit-)gegenständlichen Daten gelöscht werden müssen.

Der Beschwerdeführer wollte dies nicht akzeptieren und hielt meine Prüfung für unzureichend und erhob zunächst meinem Mitarbeiter und dann mir gegenüber Dienstaufsichtsbeschwerde. Ich habe ihn darauf hingewiesen, dass er die Beschwerde gegen mich an den zuständigen Verwaltungsrat (im vorliegenden Fall des Bayerischen Rundfunks) weiterzuleiten habe (die Dienstaufsichtsbeschwerde gegen meinen Mitarbeiter hatte ich bereits als unbegründet abgelehnt).

Es entspann sich eine Auseinandersetzung zu der Frage, ob ich die gegen mich erhobene Dienstaufsichtsbeschwerde selbst an den Verwaltungsrat weiterzuleiten hätte, was ich abgelehnt und darauf hingewiesen habe, dass es im Verantwortungsbereich des Beschwerdeführers liegt, den richtigen Adressaten für eine Dienstaufsichtsbeschwerde – ggf. auch gegen meinen Rat, den Verwaltungsrat des Bayerischen Rundfunks anzusprechen – auszuwählen. Ich habe wiederholt darauf hingewiesen, dass Dienstaufsichtsbeschwerden an die Dienstaufsicht führende Stelle zu richten seien. Der Beschwerdeführer hat sich nach einem von seiner Seite aus recht emotionalem Schriftwechsel dann offenbar entschieden, die Beschwerde nicht weiter zu verfolgen – zumindest brach der Schriftverkehr ab.

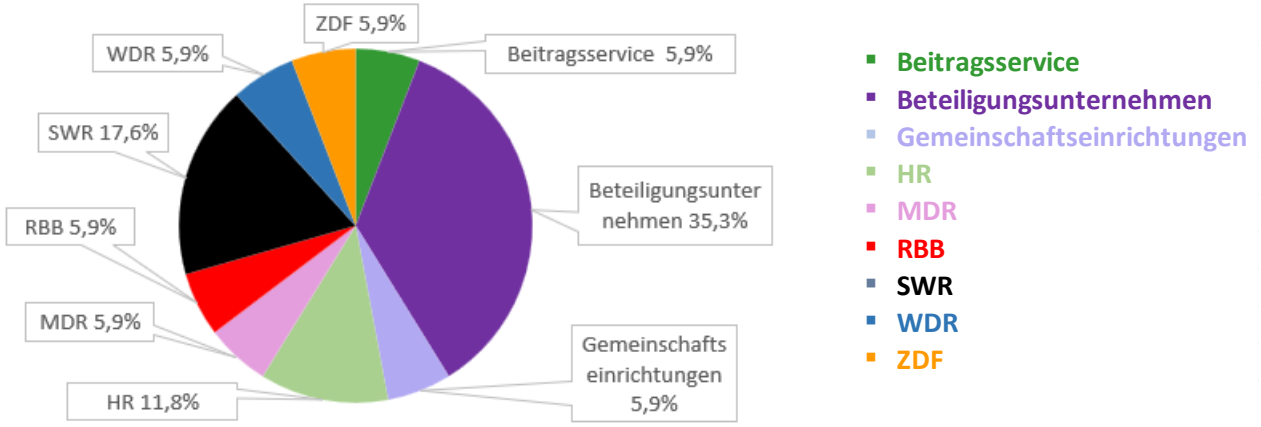
In meiner bisherigen Laufbahn ist dies die zweite gegen mich erhobene Dienstaufsichtsbeschwerde, die auch in diesem Fall erfolglos war.

5 Meldungen nach Art. 33 DSGVO

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

5.1 Meldeeingänge

18 Meldungen zu Datenschutzvorfällen gingen in unserer Aufsichtsbehörde ein. Für eine der Meldungen war unsere Zuständigkeit nicht gegeben, der Meldende hatte sich parallel bereits an die zuständige Aufsichtsbehörde des Landes gewandt. Die verbleibenden insgesamt 17 Meldungen in der Zuständigkeit des Rundfunkdatenschutzbeauftragten verteilten sich auf die beaufsichtigten Rundfunkanstalten, Beteiligungsunternehmen und Gemeinschaftseinrichtungen.



Etwa zwei Drittel der Meldungen waren mit einem Risiko oder einem hohen Risiko für die Rechte und Freiheiten betroffener Personen zu bewerten. Bei ca. einem Drittel der Meldungen war das Risiko zum Zeitpunkt der Meldung meist nicht eindeutig einschätzbar; wir begrüßen die vorsorgliche Meldung.

Datenschutzvorfälle	Anzahl gesamt	Prozent	Risikoklassifizierung	
			erhöht/hoch	gering/nicht vorh.
Beitragsservice	**1**	5,9%	1	0
Beteiligungsunternehmen	**6**	35,3%	5	1
BR	**0**	0,0%	-	-
Deutschlandradio	**0**	0,0%	-	-
Gemeinschaftseinrichtungen	**1**	5,9%	0	1
HR	**2**	11,8%	1	1
MDR	**1**	5,9%	1	0
RBB	**1**	5,9%	1	0
SR	**0**	0,0%	-	-
SWR	**3**	17,6%	1	2
WDR	**1**	5,9%	1	0
ZDF	**1**	5,9%	0	1
Gesamtergebnis	**17**	**100,0%**	**11**	**6**

Die Themen der gemeldeten Datenschutzvorfälle verteilten sich wie folgt:

Datenschutzvorfälle	Anzahl	Prozent
Hackerangriffe (Phishing/Man-in-the Middle)	4	23,5%
unzulängliche Berechtigungssteuerung	4	23,5%
digitaler Fehlversand	3	17,6%
Verlust physischer Unterlagen/Geräte	2	11,8%
Sonstige Themen	4	23,5%
Gesamtergebnis	**17**	100,0%

Fast die Hälfte aller Meldungen verteilte sich auf Hackerangriffe sowie eine unzulängliche Berechtigungssteuerung gemeinsam in der ARD genutzter Anwendungen. Dies unterstreicht den stetigen Bedarf an Sensibilisierungsmaßnahmen und geeigneten technischen und organisatorischen Vorkehrungen bei den Verantwortlichen. Ich mache an dieser Stelle auf den Tätigkeitsbericht 2025 des Hessischen Beauftragten für Datenschutz und Informationsfreiheit aufmerksam (Tätigkeitsberichte des HBDI | datenschutz.hessen.de), der auf S. 255 ff. Phishing-Angriffe unter dem Aspekt der Aufarbeitung und Prävention genauer in Augenschein nimmt.

5.2 Entwicklung der Meldungen 2023-2025

Bei der Entwicklung der Meldungen nach Art. 33 DSGVO werden die gemeldeten Vorfälle betrachtet, die in der Aufsichtstätigkeit des Rundfunkdatenschutzbeauftragten liegen.

Entwicklung 2023-2025	2023	2024		2025	
Risiko	alle	gering	erhöht/hoch	gering	erhöht/hoch
Beitragsservice	0	3	0	0	1
Beteiligungsgesellschaften	1	2	4	1	5
Gemeinschaftseinrichtungen	0	0	0	1	0
BR	3	0	2	0	0
Deutschlandradio	0	0	0	0	0
HR	0	1	0	1	1
MDR	2	0	0	0	1
RBB	0	1	0	0	1
SR	0	0	0	0	0
SWR	1	1	0	2	1
WDR	1	1	1	0	1
ZDF	2	0	2	1	0
Summe	**10**	**9**	**9**	**6**	**11**
Gesamt jährlich	**10**	**18**		**17**	

Es fällt auf, dass der Saarländische Rundfunk und Deutschlandradio in den letzten drei Berichtsjahren keinerlei (selbst nur potenziell risikobehaftete) Datenschutzvorfälle an den Rundfunkdatenschutzbeauftragten gemeldet haben. Dies kann auf sehr gut funktionierende Datenschutzprozesse hindeuten oder aber auf nicht in der erforderlichen Weise ausgestaltete Meldeprozesse. In unseren vierteljährlichen Jour fixes mit den Rundfunkanstalten haben wir diese Auffälligkeit deshalb angesprochen und eine Überwachung/Prüfung der Prozesse angeregt. Denn grundsätzlich können wir als Aufsichtsbehörde nur auf Basis der Meldung sicherheitskritischer Aspekte auch übergreifend für alle beaufsichtigten Rundfunkanstalten eine Bewertung vornehmen und diese ggf. kurzfristig informieren/sensibilisieren.

Im Ausblick auf das folgende Berichtsjahr bestätigte sich in Teilen die Annahme, dass Meldeprozesse nicht in der erforderlichen Weise ausgestaltet sein könnten. Eine vertiefte Darstellung wird im Tätigkeitsbericht 2026 erfolgen.

5.3 Verbesserungsbedarf bei Meldungen nach Art. 33 DSGVO

Datenschutzvorfälle lassen sich nicht vollständig vermeiden. Maßgeblich ist jedoch ein sachgerechter, strukturierter und rascher Umgang damit durch die Verantwortlichen, um Risiken für die Datensicherheit und den Datenschutz unverzüglich zu begrenzen und in geordnete Verfahren zu überführen. Die Aufarbeitung der gemeldeten Datenschutzvorfälle und die Kommunikation mit der Aufsichtsbehörde verliefen in der Mehrzahl der Fälle sachgerecht und konstruktiv.

5.3.1 Kommunikation mit der Aufsichtsbehörde

In einigen Fällen wurde deutlich, dass Verantwortliche und beteiligte Unternehmen die Kommunikation im Rahmen der Vorfallaufklärung nicht durchgängig sicherstellen. Verzögerte Rückmeldungen, fehlende Reaktionen zentraler Ansprechpersonen und unzureichende Stellvertretungsregelungen führten regelmäßig zu vermeidbaren Verzögerungen. Datenschutzbeauftragte sowie deren Teams müssen sich ihrer Verpflichtungen aus der DSGVO bewusst sein, insbesondere im Hinblick auf eine angemessene bzw. fristgerechte Kooperation mit der Aufsichtsbehörde.

Besonders hervorzuheben ist, dass ein Unternehmen die Einrichtung einer Stellvertretung für den Datenschutzbeauftragten aus wirtschaftlichen Gründen in Frage stellte. Wir haben hierzu klargestellt, dass zwar keine zusätzliche Stelle geschaffen werden muss, jedoch eine funktionierende Stellvertretungsregelung unverzichtbar ist. Diese hat eine vertretende Person sowie die strukturierte Übergabe relevanter Fälle zu umfassen.

Schließlich ist im Zusammenhang mit extern bestellten Datenschutzbeauftragten festzustellen, dass die Prozesse zum Umgang mit Datenschutzvorfällen in den betreuten Unternehmen verbindlich implementiert und veröffentlicht sein müssen. Nur so kann gewährleistet werden, dass interne Meldungen und externe Benachrichtigungen ordnungsgemäß und fristgerecht erfolgen.

Insgesamt zeigt sich ein deutlicher Bedarf an klareren internen Strukturen, verbindlichen Zuständigkeiten und einem präziseren Verständnis der gesetzlichen Anforderungen, um die Kommunikation mit der Aufsichtsbehörde gemäß DSGVO zuverlässig sicherzustellen.

5.3.2 Risikobewertung nach Art. 34 DSGVO

Gerade wenn Datenschutzvorfälle ggf. mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen einhergehen, sind eine schnelle Aufarbeitung und eine fundierte, nachvollziehbare Bewertung des Betroffenenrisikos nach Art. 34 DSGVO durch die Verantwortlichen essenziell. Betroffene Personen sind von der Datenschutzverletzung zu benachrichtigen, sofern diese voraussichtlich (Eintrittswahrscheinlichkeit) ein hohes Risiko für deren persönliche Rechte und Freiheiten (Schadensausmaß) zur Folge hat (vgl. Art. 34 Abs. 1 DSGVO).

Ausschlaggebend für eine Bewertung ist also eine möglichst genaue Kenntnis des Schadensausmaßes unter Einbezug aller drohenden physischen, materiellen oder immateriellen Schäden. Dabei sind insb. folgende Aspekte relevant: Art der Datenschutzverletzung, Art/Sensibilität/Umfang der personenbezogenen Daten, Identifizierbarkeit betroffener Personen, Schwere der Folgen für die betroffenen Personen, besondere Eigenschaften der betroffenen Personen oder des Verantwortlichen sowie Anzahl der betroffenen Personen. Eine Eingrenzung der Eintrittswahrscheinlichkeit wiederum könnte das Risiko des Schadensausmaßes verringern.

Wir verweisen diesbezüglich auch auf das Kurzpapier Nr. 18 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)[9], dem Anhaltspunkte zur Beurteilung des Risikos zu entnehmen sind.

Den Verantwortlichen ist zu empfehlen, einen strukturellen Rahmen für eine entsprechende Risikobewertung vorzuhalten.

5.3.3 Betroffeneninformation

Im Rahmen der Dokumentationspflichten sowie einer vollständigen und nachvollziehbaren Aktenführung fordern wir bei Datenschutzvorfällen mit hohem Risiko regelmäßig die Vorlage der

[9] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf

Betroffeneninformation an. In Einzelfällen treten hier Missverständnisse hinsichtlich des von der Aufsichtsbehörde benötigten Informationsumfangs auf. Die Nachfrage bezieht sich ausschließlich auf den konkreten Wortlaut der versendeten Information sowie die Anzahl der betroffenen Personen und das entsprechende Versanddatum. Die Übermittlung vollständiger Adress- oder Empfängerlisten ist weder erforderlich noch zulässig und würde ihrerseits eine unzulässige Weitergabe personenbezogener Daten darstellen.

6 Themen und Schwerpunkte der Aufsicht

Ein Tätigkeitsbericht soll den Leserinnen und Lesern einen Überblick darüber verschaffen, welche Schwerpunkte die Datenschutzaufsicht beschäftigt haben und welche Prioritäten gesetzt wurden. Stets bemühe ich mich, im Hinblick auf Themen der Aufsichtsbehörde eine anschauliche und möglichst interessante Auswahl zu treffen.

6.1 Prüfungen

6.1.1 Befragung zu Onboarding und Schulung

Wie bereits im letzten Tätigkeitsbericht unter Kapitel 6.5 angesprochen, wurde im Zeitraum November/Dezember 2024 eine datenschutzrechtliche Überprüfung der etablierten Prozesse zum Onboarding und zur Schulung bei den durch meine Behörde beaufsichtigten Rundfunkanstalten durchgeführt. Ausgangspunkt war, dass basierend auf den geltenden Datenschutzvorschriften ein reflektierter und strukturierter Umgang mit personenbezogenen Daten durch Beschäftigte sicherzustellen ist. Dies insbesondere im Hinblick auf

- die Erfüllung der Informationspflichten der Verantwortlichen,
- die Verpflichtung der Beschäftigten auf die Wahrung der Vertraulichkeit personenbezogener Daten/das Datengeheimnis im Rahmen des Onboardings sowie
- die Gestaltung der Datenschutz-Schulungsprozesse.

Die Überprüfung stützte sich auf eine schriftliche Befragung, deren Ergebnisse im Berichtsjahr 2025 ausgewertet und am 2. Juli 2025 an die Verantwortlichen übermittelt wurden. Die Handlungsbedarfe waren durch die verantwortlichen Stellen zu prüfen und das entsprechende Ergebnis mit einem aussagekräftigen Maßnahmenkatalog an die Aufsichtsbehörde zu übermitteln.

6.1.1.1 Informationspflichten beim Onboarding

Bei Neueinstellungen werden personenbezogene Daten in der Regel bereits vor Beschäftigungsaufnahme erhoben. Nach Art. 13 DSGVO sind gegenüber betroffenen Personen zum Zeitpunkt der Erhebung personenbezogener Daten Informationspflichten zu erfüllen. Im Rahmen des Onboardings interessierte uns, ob und wie die Information über die Datenverarbeitung bei Neueinstellungen umgesetzt wird.

Festzustellen war, dass die überwiegende Zahl der Verantwortlichen die Beschäftigten grundsätzlich über die Verarbeitung ihrer personenbezogenen Daten informiert, dass allerdings ein Verantwortlicher auch sechs Jahre nach In-Kraft-Treten der DSGVO diesbezüglich keinen Prozess aufgesetzt hatte. Weiterhin zeigte sich, dass nicht alle Verantwortlichen im Vorfeld der Datenverarbeitung informierten, sondern teilweise erst mit Aufnahme der Beschäftigung, und dass bei einigen Verantwortlichen der letzte Stand der Information (als Indiz für eine kontinuierliche Aktualisierung) nicht vermerkt war.

6.1.1.2 Wahrung der Vertraulichkeit personenbezogener Daten/Datengeheimnis

Beschäftigte sollten bei der Aufnahme ihrer Tätigkeit auf die Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten bzw. das Datengeheimnis verpflichtet werden. Ob diese Verpflichtung bei Neueinstellungen umgesetzt wird, wurde erfragt.

Mit dem Ergebnis, dass alle Verantwortlichen eine verpflichtende Erklärung zur Wahrung der Vertraulichkeit personenbezogener Daten bzw. zum Datengeheimnis einholen. Allerdings bestanden teilweise Unterschiede in Umfang (nicht alle Beschäftigtengruppen wurden durchgehend verpflichtet, ebenso ersetzt eine kurze Klausel im Arbeitsvertrag keine eigenständige Verpflichtung) und Nachweisführung (nicht alle Verantwortlichen stellten eine vollumfängliche Nachweisführung sicher). Weiterhin zeigte sich, dass bei mehreren Verantwortlichen die letzte Überprüfung und Aktualisierung über den letzten vermerkten Stand bereits älteren Datums oder durch einen nicht vermerkten Stand nicht nachvollziehbar war.

6.1.1.3 Schulungen zu Datenschutz und Informationssicherheit

Obwohl die DSGVO keine ausdrückliche Schulungspflicht für Beschäftigte vorsieht, lassen verschiedene Artikel der DSGVO den Rückschluss zu, dass Schulungen notwendig und wesentlicher Bestandteil eines wirksamen Datenschutzmanagements sind. Art. 5 Abs. 2 DSGVO verpflichtet den Verantwortlichen, die Einhaltung der Grundsätze zur Verarbeitung personenbezogener Daten sicherzustellen und deren Umsetzung nachzuweisen. Zudem fordert Art. 32 DSGVO die Implementierung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus, wozu auch die ausreichende Qualifizierung der

Mitarbeitenden zählt. Weiterhin ergibt sich aus Art. 39 Abs. 1 b DSGVO die Aufgabe des Datenschutzbeauftragten, die Sensibilisierung und Schulung der an Verarbeitungsvorgängen beteiligten Beschäftigten sowie entsprechende Überprüfungen zu überwachen.

Die Frage nach Schulungen ergab, dass die Mehrheit der Verantwortlichen verpflichtende Erstschulungen zum Datenschutz vorsieht, die meist durch webbasierte Trainings vermittelt werden. In der Regel sind definierte Zeitpunkte für die Erstschulung festgelegt, sodass neue Beschäftigte zeitnah mit den notwendigen Grundlagen vertraut gemacht werden. Unterschiede bestehen jedoch bei der Nachweisführung: Während einige Verantwortliche Teilnahmezertifikate ausstellen oder die Teilnahme durch Führungskräfte überwachen lassen, fehlt bei anderen eine systematische Kontrolle, sodass nicht nachvollzogen werden kann, ob alle Beschäftigten die Schulungen tatsächlich absolviert haben.

Erfahrungswerte zeigen, dass Beschäftigte die Verarbeitungsgrundsätze und definierte technisch-organisatorische Maßnahmen nur so gut beherzigen und anwenden können, wie sie diese (verpflichtend) kennen(lernen) und an diese regelmäßig erinnert werden. Deshalb sollten auch Folge- und Auffrischungsschulungen zum Datenschutz einen hohen Stellenwert einnehmen. Diesbezüglich bestand bei mehreren Verantwortlichen Handlungsbedarf, einen entsprechenden Prozess konkreter zu definieren und feste Intervalle sowie eine belastbare Nachweisführung aufzunehmen.

Viele Verantwortliche integrieren bereits Themen der Informationssicherheit in ihre Schulungen. Dies fördert eine ganzheitliche Sicherheitskultur und unterstützt die Beschäftigten im sicheren Umgang mit Daten.

6.1.2 Befragung zum Redaktionsdatenschutz

Journalistisch-redaktionelle Datenverarbeitungen bewegen sich in einem besonderen Spannungsfeld zwischen zwei Grundrechten, nämlich dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und der Presse- sowie Rundfunkfreiheit (Art. 5 GG). Um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen, sieht die DSGVO in Art. 85 vor, dass für die Verarbeitung zu journalistischen Zwecken die Regelungen der DSGVO nur eingeschränkt Anwendung finden[10] und die Mitgliedsstaaten Ausnahmen vorsehen. Der

[10] 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)

Medienstaatsvertrag (MStV) formuliert in §§ 12 Abs. 1 und 23 Abs. 1 das sogenannte Medienprivileg, also die entsprechende Sonderregelung zur DSGVO und adressiert diese an die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF und das Deutschlandradio.

Vor diesem Hintergrund wurde zwischen Dezember 2024 und März 2025 eine Befragung zum Redaktionsdatenschutz durchgeführt, um zu erfahren, inwieweit diese Vorschriften bei der journalistisch-redaktionellen Verarbeitung personenbezogener Daten umgesetzt und tatsächlich mit Leben erfüllt werden. Die Befragung wurde exemplarisch an zwei Redaktionsbereiche der beaufsichtigten Rundfunkanstalten, des ZDF und Deutschlandradio gerichtet (Aktuelles sowie Magazine/Hintergrund/Dokumentation), um einen möglichst repräsentativen Einblick in die redaktionelle Datenschutzpraxis zu erhalten, Optimierungschancen zu identifizieren und Handlungsempfehlungen zur Weiterentwicklung bestehender Vorgehensweisen zu geben. Die Ergebnisse der Befragung wurden im Berichtsjahr 2025 ausgewertet und am 06.11.2025 an die Verantwortlichen übermittelt.

Vor der Darstellung der Ergebnisse der Befragung soll jedoch zunächst ein rechtlicher Exkurs zu den Besonderheiten und wichtigsten Begrifflichkeiten im Rahmen der redaktionell-journalistischen Datenverarbeitung erfolgen.

6.1.2.1 Rechtlicher Exkurs zum Medienprivileg

Das **Medienprivileg** beschreibt eine gesetzlich geregelte Ausnahme für die insoweit privilegierten Medien von den allgemeinen Anforderungen des Datenschutzrechts (siehe dazu auch Kapitel 2.3, sowie ausführlich Kapitel 6.9). Um dieses Verhältnis angemessen auszubalancieren, sieht der Medienstaatsvertrag (MStV) in §§ 12 Abs. 1 und 23 Abs. 1 entsprechende Sonderregelungen vor.

- Das **Datengeheimnis** bezeichnet die gesetzlich verankerte Pflicht, personenbezogene Daten, die zu journalistischen Zwecken verarbeitet werden, ausschließlich in diesem Rahmen zu verwenden (Zweckbindung). Personen, die mit solchen Daten arbeiten, sind gemäß §§ 12 Abs. 1 S. 2 und 23 Abs. 1 S. 2 MStV auf das Datengeheimnis zu verpflichten. Diese Verpflichtung gilt auch über das Ende der Tätigkeit hinaus.
- Gemäß Art. 24 und 32 DSGVO wird unter **Datensicherheit** der Datenschutz durch Technikgestaltung (geeignete technische und organisatorische Maßnahmen) verstanden, der unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ein dem Risiko angemessenes Schutzniveau gewährleistet. Datensicherheit ist die praktische Umsetzung des Schutzes digitaler Informationen gegen unbefugten Zugriff, Beschädigung oder Diebstahl. §§ 12 und 23, jeweils Abs. 1 Satz 4 MStV sehen ausdrücklich vor, dass diese Vorgaben auch bei journalistischer Datenverarbeitung

einzuhalten sind. Auch wird an der gleichen Stelle auf Art. 5 Abs. 1 lit. f der DSGVO verwiesen, der jegliche Datenverarbeitung von personenbezogenen Daten auf die Grundsätze der Vertraulichkeit und Integrität verpflichtet.

Entscheidend für die Anwendung des Medienprivilegs ist, ob die Datenverarbeitung einem „journalistischen Zweck“ dient (siehe Kapitel 6.9). Die nachfolgenden Beispiele sollen die Anwendbarkeit des Medienprivilegs im Hinblick auf die Datenverarbeitungen einer Redaktion verdeutlichen.

Medienprivileg anwendbar (ausreichender journalistischer Zweck)

- Recherche und dafür erforderliche Kommunikation (E-Mails, Social-Media, usw.), Notizen, Kalendereinträge usw.
- Reisedaten in Verbindung mit Recherche und Beitragserstellung
- Vertragsdaten mit Protagonisten und anderen bei der Herstellung von journalistischen Inhalten Beteiligten
- Programmbeschwerden
- Medienarchive

Medienprivileg nicht anwendbar (kein journalistischer Zweck)

- Personaldatenverarbeitung
- Datenverarbeitung für den Rundfunkbeitragseinzug
- Akquise von Abonnenten
- Kommerzielle Weitergabe an Dritte – Werbezwecke oder Suchmaschinen
- Datenweitergabe zu privaten Zwecken
- Datenverarbeitung zum Bezug von Newslettern
- Nutzungsmessung

Für eine Datenverarbeitung ohne journalistischen Zweck muss für eine rechtmäßige Verarbeitung eine Rechtsgrundlage gemäß Art. 6 DSGVO vorhanden sein.

Nachfolgend werden die Ergebnisse der Befragung dargestellt.

6.1.2.2 Datengeheimnis – Sicherstellung der Zweckbindung

Von Interesse war, wie in den Redaktionen sichergestellt wird, dass das Datengeheimnis beachtet und umgesetzt wird. Das Gesetz sieht hier eine Verpflichtung der mit der Verarbeitung personenbezogener Daten zu journalistischen Zwecken befassten Personen auf das Datengeheimnis bei Aufnahme der Tätigkeit vor, welches auch nach Beendigung der Tätigkeit fortbesteht.

Als wesentliche Maßnahmen wurden vor allem die schriftliche Verpflichtung auf das Datengeheimnis, der Verweis auf geltende interne Vorgaben sowie Schulungen zu Datenschutz und Informationssicherheit genannt. Gleichzeitig zeigte sich, dass die Verpflichtung auf das Datengeheimnis nicht in allen Redaktionen konsistent sowohl für feste als auch für freie Mitarbeitende umgesetzt wird. Daraus ergab sich als zentrale Optimierungschance, den Verpflichtungsprozess vollständig, einheitlich und nachweisbar für alle Personengruppen zu etablieren; zur Unterstützung wurde eine „Checkliste zur Umsetzung der Verpflichtung auf das Datengeheimnis“ durch den Rundfunkdatenschutzbeauftragten bereitgestellt.

Im Hinblick auf eine Grundsensibilisierung zum Datenschutz und zur Informationssicherheit wurde deutlich, dass diese in einem großen Teil der Redaktionen bereits stattfindet, oft sogar verpflichtend für feste und freie Mitarbeitende ist. Da fehlende Schulungen das Sicherheitsrisiko erhöhen, ist eine standardisierte Grundsensibilisierung für neue Mitarbeitende grundsätzlich anzuraten, idealerweise verbunden mit einer Einordnung der Grundlagen des Medienprivilegs. Um den Redaktionen eine Überprüfung und Optimierung des bestehenden Vorgehens zu erleichtern, wurde eine „Checkliste zur Grund- und Folgeschulung Datenschutz und Medienprivileg Datensicherheit“ an die Rundfunkanstalten ausgereicht.

Zudem legten die Antworten nahe, dass im Rahmen der Sensibilisierung klar zwischen übergreifend geltenden Standardprozessen und redaktionsspezifischen Verfahren, die unmittelbar der Umsetzung des Datengeheimnisses und der Datensicherheit dienen, unterschieden werden sollte. Deshalb wurde ein spezifisches redaktionelles Onboarding als verbindlicher Dreh- und Angelpunkt für die Einweisung neuer Mitarbeitender empfohlen. Zur Überprüfung und Weiterentwicklung bestehender Prozesse wurden beispielhafte „Muster-Inhalte für ein Onboarding redaktioneller Mitarbeitender“ zur Verfügung gestellt.

6.1.2.3 Datengeheimnis – Regelungen zu und Umgang mit Verstößen

Selbst wenn organisatorische Rahmenbedingungen zur Sicherstellung der Beachtung und Umsetzung des Datengeheimnisses bestehen, kann es zu Verstößen kommen. Uns interessierte, ob in den Redaktionen Regelungen zum Datengeheimnis und zum Umgang mit Verstößen dagegen vorliegen und wie im Ereignisfall mit solchen Verstößen umgegangen wird. Die Antworten zeigten,

dass in allen Redaktionen grundsätzlich Regelungen vorhanden sind, die jedoch in unterschiedlicher Tiefe und Klarheit übermittelt wurden; teilweise waren sie zudem mit Themen wie Persönlichkeitsrechtsverletzungen oder allgemeinen Datenschutzvorfällen vermischt. Den Redaktionen wurde deshalb die Handlungsempfehlung gegeben, das Datengeheimnis sowohl präventiv als auch reaktiv zu betrachten: Präventiv sollte der Umgang mit journalistischen Daten im Sinne des Datengeheimnisses klar geregelt sein, während im Fall eines tatsächlichen Verstoßes ein strukturierter Ablauf zur kurzfristigen und effektiven Schadensbegrenzung greifen muss. Um die Redaktionen dabei zu unterstützen, die bestehenden Regelungen zu prüfen, zu schärfen und weiterzuentwickeln, wurde eine „Checkliste zu Regelungen rund um das Datengeheimnis“ bereitgestellt.

6.1.2.4 Datensicherheit – Maßnahmen und eingesetzte Tools

Gemäß Art. 24 und 32 DSGVO wird unter Datensicherheit der Datenschutz durch Technikgestaltung (geeignete technische und organisatorische Maßnahmen) verstanden, der unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ein dem Risiko angemessenes Schutzniveau gewährleistet (z.B. durch sichere Infrastruktur, Pseudonymisierung, Verschlüsselung, Löschung, Berechtigungskonzept etc.).

Von Interesse war deshalb, welche technischen und organisatorischen Maßnahmen in den Redaktionen als wesentlich angesehen werden, um den Anforderungen an die Datensicherheit bei journalistischer Tätigkeit gerecht zu werden. Darüber hinaus sollte ein erstes Bild der Zusammenhänge zwischen genutzten Diensten/Tools und redaktionellen Arbeitsprozessen bzw. Zwecken gewonnen werden. Die Antworten waren insgesamt vielfältig in Umfang und Tiefe und erlaubten einen ersten Eindruck, in welchem Umfang eine redaktionelle Sicherheitskultur bereits etabliert ist.

Als wesentlich erachtet wurden sowohl allgemein in der Rundfunkanstalt geltende Prozesse und Vorgehensweisen als auch redaktionsspezifische technische und organisatorische Vorkehrungen, um speziell den Anforderungen bei der journalistischen Tätigkeit gerecht zu werden. Vor dem Hintergrund der Haftung für unzureichende Sicherheitsmaßnahmen im Redaktionsdatenschutz wurde generell empfohlen, die bestehenden Maßnahmen zur Datensicherheit zu überprüfen, zu optimieren und kontinuierlich weiterzuentwickeln. Den Redaktionen wurde hierfür eine prozessorientierte Kurz-Checkliste zur „Festlegung von Datensicherheitsmaßnahmen für die journalistische Tätigkeit“ zur Verfügung gestellt.

Die Informationen zu den übermittelten Tools und Diensten, die in der journalistischen Arbeit genutzt werden, ermöglichten ein grobes Bild der Zusammenhänge zwischen eingesetzten Lösungen und redaktionellen Prozessen. Für einen dauerhaft aktuellen Überblick über die genutzten Dienste/Tools im Hinblick auf die Datensicherheitsaspekte wurde empfohlen, eine fortzuschreibende Übersicht in den Redaktionen vorzuhalten, die Tool/Dienst, Zweck, verarbeitete Daten sowie zusätzliche technisch-organisatorische Maßnahmen zusammenführt. Beispielhaft wurde dafür eine Vorlage zur Überprüfung und Dokumentation der Dienste und Tools an die Redaktionen ausgegeben.

Gerade für streng vertrauliche, kritische oder sensible Daten – wie sie insbesondere im investigativen Journalismus vorkommen – bestehen erhöhte Anforderungen an die Datensicherheit (Informantenschutz). Zwar wurden hierfür zahlreiche Einzelmaßnahmen benannt, jedoch konnte kein vollständiges Bild eines umfassend durchdachten Maßnahmenpaketes vermittelt werden. Da die notwendigen Maßnahmen zur Datensicherheit anhand erkannter Risiken gewählt und umgesetzt werden sollten, wurde empfohlen – sofern noch nicht geschehen – die Auswahl der Schutzmaßnahmen auf eine solide Grundlage zu stellen: Zunächst sollte eine Datenklassifizierung und Risikobetrachtung verarbeiteter Datenkategorien vorgenommen werden, um darauf aufbauend risikomindernde Maßnahmen zu definieren und zu einer vollumfänglichen Schutzstrategie zu entwickeln und diese fortzuschreiben.

6.1.2.5 Einbeziehung des internen Datenschutzes

Datenschutzbeauftragte bzw. Datenschutzkoordinatoren sind bei den Verantwortlichen die Anlaufstellen für datenschutzrechtliche Themen und Fragen. Von Interesse war deshalb, wie sich die Zusammenarbeit zwischen Redaktionen und Datenschutz gestaltet. Es zeigte sich, dass diese überwiegend anlassbezogen erfolgt. Um Datenschutz und Datensicherheit kontinuierlich im redaktionellen Alltag zu verankern und eine dauerhafte Präsenz der Thematik sicherzustellen, wurde den Redaktionen empfohlen, dieses Vorgehen um regelmäßige Austauschformate zu ergänzen.

6.1.2.6 Datenschutzvorgaben für Mitarbeitende

Gegenstand der Befragung war, ob und welche Datenschutzvorgaben für die journalistische Arbeit existieren und wie der Zugriff darauf für feste und freie Mitarbeitende sichergestellt wird. In allen Redaktionen lagen vielfältige Vorgaben vor. Da die Wirksamkeit maßgeblich davon abhängt, ob diese Vorgaben zur richtigen Zeit, über geeignete Kanäle und für alle Zielgruppen zugänglich gemacht werden, wurde eine Überprüfung von Optimierungspotenzialen diesbezüglich empfohlen. Es sollte klar definiert sein, welche Vorgaben in welcher Form bereitgestellt werden, wann sie im Arbeitsprozess vermittelt werden und wie Mitarbeitende sie im Alltag schnell und unkompliziert

finden und nutzen können, damit die bestehenden Regelungen tatsächlich in die tägliche Arbeit einbezogen werden.

6.1.3 Geplante Prüfungen für das nächste Berichtsjahr

Meiner Aufsicht unterliegen sowohl die Rundfunkanstalten, als auch deren mehrheitlich im öffentlich-rechtlichen Rundfunk beteiligten Unternehmen sowie deren Gemeinschafts-einrichtungen.

Im Jahr 2026 und im Hinblick auf die Erweiterung der Aufsichtstätigkeit auf alle Landesrundfunkanstalten der ARD, ZDF und Deutschlandradio sieht meine Aufsichtsbehörde eine Querschnittsprüfung der Beteiligungsunternehmen vor. Im Berichtsjahr wurde deshalb im ersten Schritt damit begonnen, auf unserer Website ein Meldeformular für Datenschutzbeauftragte zu hinterlegen und die vorliegende Datenbasis zu schärfen, um dann 2026 die neu zu beaufsichtigenden Verantwortlichen zu ergänzen.

Weiterhin geplant ist eine Prüfung zum Personaldatenschutz, die an die Rundfunkanstalten, das ZDF und Deutschlandradio gerichtet sein soll. Betrachtet werden soll die Verarbeitung personenbezogener Daten im Zusammenhang mit der Anbahnung, Durchführung und Beendigung eines Beschäftigungsverhältnisses.

6.2 Handreichung zu Aufbau und Weiterentwicklung eines DSMS

Ein Datenschutzmanagementsystem (DSMS) bündelt alle relevanten Vorgaben und Informationen zum Datenschutzmanagement, ermöglicht die Überprüfung von dessen Wirksamkeit und unterstützt dabei, der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO Genüge zu tun.

Als Kernelemente eines DSMS greifen eine Datenschutzleitlinie (interne Vorgaben mit Zielbild, Grundsätzen, Rollen und Verantwortlichkeiten), Datenschutzrichtlinien (Ausgestaltung von Datenschutzprozessen) und deren wiederkehrende Wirksamkeitsprüfung (kontinuierliche Verbesserung) ineinander. Ein Datenschutzleitfaden als wegweisendes Rahmenwerk umschließt diese und bündelt alle relevanten Vorgaben, Informationen, Dokumente und Aufzeichnungen, um so einen schnellen und übersichtlichen Zugriff darauf zu ermöglichen.

Um die durch uns beaufsichtigten Rundfunkanstalten bei Aufbau und Weiterentwicklung eines Datenschutzmanagementsystems (DSMS) zu unterstützen, stellten wir diesen die im Berichtsjahr entwickelte Handreichung „Datenschutzmanagement-Check“ sowie begleitende Checklisten bereit.

An den eigenen Stand der jeweiligen Prozesse anknüpfend und mit der Handreichung als Hilfsmittel können die Verantwortlichen so ihr DSMS weiter aufbauen und vervollständigen.

Die Handreichung umfasst drei Checklisten, die sich in einer zugehörigen Excel-Tabelle wiederfinden und Entwicklungen über die Zeit nachvollziehbar machen sollen:

- Datenschutzmanagement: Ausprägung reaktiv bzw. proaktiv
- Datenschutzprozesse: Reifegradeinstufung der Einzelprozesse
- Datenschutzmanagementsystem: Entwicklungsstand der Kernelemente eines DSMS

Nach einer einmaligen Bestandsaufnahme können und sollen diese als ein lebendiges Steuerungsinstrument und eine Nachweisführung bis hin zu einem wirksamen DSMS genutzt werden.

Ergänzend wurde im Berichtsjahr empfohlen – falls noch nicht geschehen – die Rolle des Datenschutzkoordinators im Rahmen der strategischen Steuerung eines DSMS einzuführen. Die Datenschutzkoordinatoren stärken die Datenschutzorganisation insgesamt (Bindeglied zwischen dem zentralen Datenschutz und den Fachabteilungen) und minimieren dadurch Risiken von Datenschutzverstößen.

6.3 Aufzeichnung von Personalversammlungen

Im Berichtszeitraum hat die RDSK die Frage bewertet, ob Personal- bzw. Betriebsversammlungen bei den öffentlich-rechtlichen Rundfunkanstalten aufgezeichnet werden dürfen und auf welcher Grundlage dies rechtmäßig möglich wäre. Das Ergebnis lässt sich kurz zusammenfassen: In den meisten Anstalten sind Aufzeichnungen gesetzlich ausgeschlossen; zulässige Ausnahmen bestehen nur für Radio Bremen und den SWR, dort aber ausschließlich mit Einwilligung der Teilnehmenden oder auf Basis einer entsprechenden Dienstvereinbarung.

Rechtlich ist zu unterscheiden: Das Betriebsverfassungsgesetz (BetrVG) gilt nur für private Unternehmen und nicht für die Rundfunkanstalten; für letztere greifen das Bundespersonalvertretungsgesetz (BPersVG) oder die jeweiligen Landespersonalvertretungsgesetze (LPersVG). Während das BetrVG nach Wegfall der pandemiebedingten Sonderregelung keine virtuellen Betriebsversammlungen mehr vorsieht, ist dies für den Rundfunk ohne Belang; maßgeblich ist hier vielmehr der Grundsatz der Nichtöffentlichkeit, also die Beschränkung der Teilnahme auf den Dienststellenkreis, der auch bei

Videoübertragungen strikt einzuhalten ist (z. B. durch rein interne, nicht frei zugängliche Übertragung und sichere Identitätsprüfung).

Nach § 58 Abs. 1 S. 3 i. V. m. § 38 Abs. 3 S. 3 BPersVG („Eine Aufzeichnung ist unzulässig.“) sind Aufzeichnungen generell verboten; diese Vorgabe gilt u. a. für NDR, rbb und MDR kraft der jeweiligen Staatsverträge. Entsprechende Verbote finden sich zudem in mehreren Landesgesetzen (etwa in NRW, Bayern, Hessen, Saarland, Rheinland-Pfalz). Für Radio Bremen (Bremisches Personalvertretungsgesetz) und den SWR (LPVG Baden-Württemberg) fehlt hingegen ein ausdrückliches Aufzeichnungsverbot; dort kommt eine Aufzeichnung nur in Betracht, wenn datenschutzrechtliche Voraussetzungen strikt beachtet und eine tragfähige Rechtsgrundlage geschaffen wird.

Datenschutzrechtlich gilt: Der Zweck der Aufzeichnung muss eng gefasst sein (z. B. zeitlich befristete Nachsicht für Verhinderte oder reine Gedächtnisstütze für die Protokollführung); beide Zwecke unterscheiden sich in der Eingriffsintensität erheblich. Daraus folgen strenge Speicherbegrenzungen (Löschung nach Zweckerreichung) sowie umfassende Transparenz- und Informationspflichten gegenüber allen Teilnehmenden (Art. 12, 13 DSGVO). Als Rechtsgrundlage kommen realistisch nur zwei Wege in Betracht: (1) die Einwilligung aller identifizierbaren Teilnehmenden (schriftlich/elektronisch, in der Praxis organisatorisch oft aufwendig) oder (2) eine Dienstvereinbarung zwischen Dienststelle und Personalrat, gestützt auf Art. 88 DSGVO und die einschlägigen landesrechtlichen Beschäftigtendatenschutz-Regelungen; eine bloße Dienstanweisung genügt nicht. Andere Grundlagen – insbesondere „berechtigte Interessen“ nach Art. 6 Abs. 1 lit. f DSGVO – scheiden regelmäßig aus, weil der anhaltende Effekt einer Aufzeichnung die Persönlichkeitsrechte der Beschäftigten in der Abwägung überwiegt.

In der Bewertung wird betont, dass Aufzeichnungen das Risiko einer unkontrollierten Vervielfältigung oder Verfälschung erhöhen und die Nichtöffentlichkeit schwerer sicherzustellen ist. Als mildere Mittel werden deshalb Protokolle oder interne Zusammenfassungen empfohlen, um verhinderten Beschäftigten die Inhalte der Versammlung zugänglich zu machen, ohne in Grundrechte stärker einzugreifen. Insgesamt bleibt es damit dabei: Für die meisten Rundfunkanstalten sind Aufzeichnungen unzulässig; wo sie nicht ausdrücklich verboten sind, kommen sie nur ausnahmsweise und unter strengen Datenschutzvorkehrungen in Betracht.

6.4 Datensicherheit in der Aufsichtstätigkeit

Datensicherheit bildet einen zentralen Baustein der datenschutzrechtlichen Aufsicht, weil sie den praktischen Schutz personenbezogener Daten gewährleistet und damit die Wirksamkeit sämtlicher

Datenschutzgrundsätze erst ermöglicht. Auch im medienprivilegierten Bereich (vgl. §§ 12, 23 MStV) – das heißt dort, wo die inhaltliche journalistische Arbeit weitgehend von der Anwendung der DSGVO ausgenommen ist – bleibt Art. 32 DSGVO in vollem Umfang anwendbar. Die Anforderungen an technische und organisatorische Maßnahmen (TOM) sowie der Grundsatz der Integrität und Vertraulichkeit gelten damit fort.

In der Aufsichtspraxis des Rundfunkdatenschutzbeauftragten zeigt sich, dass Fragen der Datensicherheit regelmäßig unmittelbarer Anlass für Beratungen, Prüfungen oder Meldungen von Datenschutzverletzungen (Art. 33 DSGVO - siehe Kapitel 5) sind. Gerade Rundfunkanstalten betreiben komplexe IT-Infrastrukturen mit Redaktionssystemen, Produktionsnetzwerken, mobilen Arbeitsprozessen, cloudbasierten Kollaborationstools und Datenarchiven. Diese Umgebungen sind vielfältigen Risiken ausgesetzt – von unzureichend gehärteten Systemen über Sicherheitslücken in Drittsoftware bis hin zu Angriffen auf mobile Endgeräte.

Ein Blick in die Tätigkeitsberichte anderer Datenschutzaufsichten zeigt, dass Datensicherheit bundesweit eines der dominierenden Themenfelder ist und häufig auch Gegenstand vertiefter technischer Prüfungen wird. Regelmäßig wird über Fälle, in denen unverschlüsselte Datenträger, fehlende Multi-Faktor-Authentifizierung oder unsichere mobile Arbeitsumgebungen zu Datenschutzproblemen geführt haben, berichtet. Solche Fallkonstellationen finden sich in ähnlicher Weise auch im Umfeld von Rundfunkanstalten und Beteiligungsunternehmen.

Die Berichte zeigen, dass mangelnde Verschlüsselung, fehlerhafte Backup-Konzepte, Klartextpasswörter, fehlende Sicherheitsupdates und unzureichende Notfallpläne zu den wiederkehrenden Befunden gehören. Hier gilt es regelmäßig durch die IT-Sicherheit und den Datenschutz gleichermaßen die Verantwortlichen darüber zu sensibilisieren, um aus eigenen oder auch aus Fehlern anderer zu lernen.

Diese Beobachtungen spiegeln Risiken wider, die auch für die Rundfunkanstalten relevant sind. So erfordern etwa cloudbasierte Produktionsprozesse, hybride Redaktionsumgebungen oder digitale Archivsysteme ein besonderes Augenmerk hinsichtlich Verschlüsselung, Zugriffskonzepten und Rechteverwaltung. Auch die Tatsache, dass die journalistische Arbeit zunehmend mobil erfolgt, verstärkt die Bedeutung sicherer Endgeräte, sicherer Kommunikationswege und robuster Backup-Strategien. Datenschutzrechtliche Vorgaben wie Art. 32 DSGVO wirken hier als Mindeststandard, der zugleich im Interesse der Rundfunkanstalten selbst liegt: Ein erfolgreicher Angriff auf Produktionssysteme, Archive oder Rechercheinhalte hätte nicht nur datenschutzrechtliche, sondern auch erhebliche betriebliche und medienethische Auswirkungen.

Für die Aufsicht bedeutet dies, dass Datensicherheit in mehreren Dimensionen in die Tätigkeit hineinwirkt:

- **Beratung und Sensibilisierung** zu sicherer Systemkonfiguration, Verschlüsselung, Zugriffsmanagement, Cloud-Nutzung und Notfallvorsorge.
- **Reaktion auf und Bewertung von Datenschutzverletzungen**, insbesondere nach Cyberangriffen, technischen Störungen oder Fehlkonfigurationen.
- **Beobachtung technologischer Entwicklungen**, etwa im Bereich KI, Cloud-Souveränität, mobile Arbeitsprozesse oder sicherheitsrelevanter Software-Standards.

Gerade im journalistischen Bereich ist der Schutz der Datenintegrität und -verfügbarkeit von besonderer Relevanz. Angriffe auf Redaktionssysteme können nicht nur personenbezogene Daten gefährden, sondern auch die Funktionsfähigkeit der Rundfunkanstalt und damit die Rundfunkfreiheit beeinträchtigen. Datensicherheit erhält dadurch eine verfassungsrechtliche Schutzdimension, die über das rein Datenschutzrechtliche hinausgeht.

Insgesamt zeigt sich, dass Datensicherheit ein durchgehend präsentes und wachsendes Handlungsfeld im Rahmen der Aufsichtstätigkeit des Rundfunkdatenschutzbeauftragten darstellt. Der Vergleich mit anderen Datenschutzaufsichten verdeutlicht, dass viele Herausforderungen – von unzureichender Systemhärtung bis hin zu Cloud-Komplexität und Cyberangriffen – sektorenübergreifend auftreten. Auch dafür ist es erforderlich, dass die Aufsichtsbehörde mit den erforderlichen Kapazitäten ausgestattet ist (siehe auch Schlussbemerkung, Kapitel 12), um diesen zunehmenden Herausforderungen mit Schlagkraft zu begegnen.

6.5 Notwendigkeit einer Wiederholung der Verpflichtung auf das Datengeheimnis?

Nach den §§ 12 und 13 des Medienstaatsvertrages müssen alle Journalisten auf das Datengeheimnis, also die Untersagung, journalistische Daten zu anderen Zwecken zu verwenden, hingewiesen und verpflichtet werden (siehe auch Kapitel 6.1.2 zur Befragung Redaktionsdatenschutz). Aus dem Bayerischen Rundfunk erreichte mich die Anfrage, ob aus Sorgfaltsgründen und um dieses Thema ständig im Bewusstsein der Mitarbeitenden zu halten, eine regelmäßige Erneuerung dieser Verpflichtung vorgenommen werden sollte.

Zunächst habe ich darauf hingewiesen, dass sich Vorgaben zu einer regelmäßigen Wiederholung einer Verpflichtung auf das Datengeheimnis weder im nationalen noch im europäischen Recht finden. Es geht nach meiner Einschätzung um die Umsetzung der Rechenschaftspflicht aus

Art. 5 Abs. 2 DSGVO, insofern hat der Verantwortliche hier einen gewissen Ermessensspielraum. Ich habe darauf hingewiesen, dass alle Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten betraut sind, auch jenseits der medienstaatsvertraglichen Vorgaben bei der Aufnahme der Beschäftigung auf die Vertraulichkeit verpflichtet werden. Regelmäßige Schulungen und Sensibilisierungen in Hinblick auf die Einhaltung des Datengeheimnisses bzw. die Vorgaben der DSGVO sind insgesamt zielführend und erscheinen auch ausreichend. Eine wiederholte Unterzeichnung einer Verpflichtungserklärung kann aus meiner Sicht keine erhöhte Wirksamkeit entfalten; erfolgte Schulungen und Sensibilisierungsmaßnahmen sollten allerdings dokumentiert werden. Der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO kann der Verantwortliche auch so nachkommen. Die sehr aufwendige und aus meiner Sicht lediglich aus formalen Gründen zu fordernde Wiederholung einer Verpflichtung kann damit unterbleiben.

6.6 WhatsApp als Kommunikationsweg

Bereits im Tätigkeitsbericht über das Jahr 2024 hatte ich unter Kapitel 6.13 angemerkt, dass der Einsatz von WhatsApp als Kommunikationskanal zwischen Nutzenden und öffentlich-rechtlichem Rundfunk gelegentlich als kritisch angesehen wird.

Auch im Berichtsjahr 2025 wurde ich mit insgesamt drei Beschwerden zu diesem Thema konfrontiert.

Stets kann ich die grundsätzlich ablehnende Haltung zu diesem Messenger gut nachvollziehen und weise auf den vorzugswürdigen Einsatz datenschutzfreundlicher Alternativen hin. Das Argument, dass der öffentlich-rechtliche Rundfunk sein Angebot über vorhandene Wege verbreiten muss, ist nach wie vor gültig und aus meiner Sicht auch richtig. Die Nutzung von WhatsApp steht allen frei, es muss aber auch – und auch darauf mache ich beständig aufmerksam – die Möglichkeit von alternativen Kommunikationswegen bestehen. Diese Forderung wird stets umgesetzt: Niemand, der mit einer Rundfunkanstalt, dem ZDF oder Deutschlandradio Kontakt aufnehmen will, ist auf WhatsApp angewiesen. Die Forderung nach digitaler Souveränität und damit der erstrebenswerten Unabhängigkeit von US-amerikanischen Großkonzernen bleibt auch in Ansehung der publizistischen und strukturellen Unabhängigkeit des öffentlich-rechtlichen Rundfunks in Deutschland von großer Bedeutung. Als Rundfunkdatenschutzbeauftragter sehe ich mich in der Verantwortung und Pflicht, auf das mittel- bis langfristige Ziel der Umsetzung von digitaler Souveränität hinzuweisen und deren Wichtigkeit zu betonen. Hierzu bedarf es der Anstrengung nicht nur der Rundfunkanstalten, sondern auch der Politik und mein Eindruck ist, dass dies im Wesentlichen auch wahrgenommen und verstanden wird.

6.7 Sammelbeschwerde Videoüberwachung

Das Thema Videoüberwachung rückte, ausgelöst durch eine umfassende Beschwerde zu Videoüberwachungsmaßnahmen an diversen Standorten der Rundfunkanstalten, im Berichtsjahr in den Fokus. Auch wenn eine unmittelbare Betroffenheit der Beschwerde führenden Person an den Standorten größtenteils nicht festgestellt werden konnte, so habe ich die Beschwerde zum Anlass genommen, die Videoüberwachung unter datenschutzrechtlichen Gesichtspunkten zu überprüfen.

Es konnte u. a. flächendeckend festgestellt werden, dass eine dauerhafte Aufzeichnung der Kameraaufnahmen nicht erfolgt, und der Zugriff auf die Live-Bilder in Video-Katastern detailliert geregelt ist. Zweck der Videoüberwachungsmaßnahmen ist standortunabhängig ausschließlich der jeweilige Objektschutz.

Im Schwerpunkt wurde die Positionierung der Kameras sowie die Einhaltung der Informationspflichten (Hinweisschilder, Erreichbarkeit weiterer Informationen) in den Blick genommen.

Zu den Mindestanforderungen, die Art. 13 Abs. 1 und 2 DSGVO aufstellen, gehört zunächst ein klar erkennbarer Hinweis auf die Beobachtung, etwa durch ein Piktogramm oder ein Kamerasymbol. Zudem müssen sowohl die Identität und die Kontaktdaten der verantwortlichen Stelle als auch – sofern vorhanden – die Kontaktdaten der/des betrieblichen Datenschutzbeauftragten angegeben werden. Weiterhin sind die Zwecke der Verarbeitung und ihre Rechtsgrundlage in knapper Form zu benennen; stützt sich die Verarbeitung auf ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO, ist auch dieses konkret zu erläutern. Zusätzlich ist die Speicherdauer der Aufnahmen anzugeben. Abschließend muss darauf hingewiesen werden, wo die betroffenen Personen sämtliche weiteren Pflichtinformationen nach Art. 13 DSGVO – etwa zu Auskunfts- und Beschwerderechten oder zu möglichen Empfängern der Daten – einsehen können.

Wie im Rahmen unserer Prüfung festgestellt wurde, enthielten die Hinweise einiger Rundfunkanstalten jedoch nicht alle erforderlichen Informationen. Die jeweils identifizierten Mängel konnten mit Unterstützung der betrieblichen Datenschutzbeauftragten in der Folge behoben werden. In Einzelfällen wurden Ausrichtung oder Einstellungen von Kameras angepasst sowie in mehreren Fällen Positionierung und Inhalt von Hinweisschildern verbessert mit dem Ziel einer zweifelsfreien Datenschutzkonformität. Da die festgestellten Verstöße gegen die Informationspflichten aus der DSGVO durch die Anstalten kurzfristig behoben werden konnten, habe ich von weiteren aufsichtsrechtlichen Maßnahmen abgesehen.

Bei der Beschaffung, Einrichtung und dem Betrieb von Videoüberwachungssystemen ist stets auf eine sichere Ausgestaltung gemäß Art. 32 DSGVO sowie auf eine datenschutzfreundliche Technikgestaltung im Sinne von Art. 25 DSGVO zu achten. Der Verantwortliche hat insbesondere zu prüfen, ob der Einsatz der Videoüberwachung zeitlich begrenzt werden kann und welche Bereiche der Kamera erfasst werden müssen oder – etwa durch Ausblendungen oder Verpixelungen – reduziert werden können.

Die datenschutzrechtlichen Anforderungen an Videoüberwachungsmaßnahmen bleiben damit ein Thema, das regelmäßig durch die Verantwortlichen überprüft und bei Installation neuer Kameras von Anfang an mitbedacht werden muss.

6.8 Künstliche Intelligenz

Auch im Berichtsjahr 2025 war das Thema Künstliche Intelligenz prägend für die datenschutzrechtliche Arbeit der Rundfunkanstalten. Die Entwicklungen der vergangenen zwei Jahre zeigen deutlich, dass KI-Systeme nicht nur technologische Innovation ermöglichen, sondern auch zunehmend komplexe datenschutzrechtliche und regulatorische Fragestellungen aufwerfen. Wo KI im Einsatz ist, werden Daten verarbeitet – häufig personenbezogene oder personenbeziehbare Daten –, und damit steigen die Anforderungen an Rechtmäßigkeit, Transparenz und technische Sicherheit weiter an.

Eine der größten Herausforderungen bleibt dabei die Frage nach dem Personenbezug im Kontext von Trainingsdaten, Modellarchitekturen und KI-Outputs. Ein Personenbezug in KI-Modellen lässt sich oft nicht abschließend verneinen, weil Modelle auch ohne explizite Speicherung von Trainingsdaten Informationen memorieren oder ableiten können. Dies wirkt sich unmittelbar auf die Anwendbarkeit der DSGVO aus, die auch im neuen KI-Regulierungsumfeld unverändert vollständig gilt.

Die im Jahr 2024 in Kraft getretene KI-Verordnung (KI-VO) (siehe Kapitel 3.2) verfolgt ein anderes Regelungsziel als die DSGVO: Sie ordnet KI-Systeme nach Risikoklassen ein und stellt Anforderungen an Sicherheit, Governance und technische Robustheit. Gerade deshalb entstehen in der Praxis Schnittstellenprobleme zwischen KI-VO und DSGVO, etwa bei der Frage, ob KI-Systeme personenbezogene Daten verarbeiten, wie Betroffenenrechte umgesetzt werden können oder welche Rolle die KI-Kompetenz des verantwortlichen Personals spielt.

Eine wesentliche Neuerung des Jahres 2025 war das Inkrafttreten der Pflicht zur KI-Kompetenz nach Art. 4 KI-VO zum 2. Februar. Anbieter und Betreiber von KI-Systemen – einschließlich

öffentlich-rechtlicher Rundfunkanstalten – müssen nun nachweisbar sicherstellen, dass Mitarbeitende über ein angemessenes Maß an Wissen und Fähigkeiten zur sachkundigen Nutzung von KI verfügen. Zwar sind keine formalen Zertifizierungen vorgeschrieben, der Kompetenzaufbau muss jedoch rollenbezogen, kontextabhängig und vor allem dokumentiert erfolgen. Um dies zu erreichen, bieten die Anstalten zum Beispiel die allgemeine Schulung für einen „KI-Führerschein“ an.

In den Rundfunkanstalten selbst hat der Einsatz von KI weiter an Bedeutung gewonnen. Neben der Entwicklung anstaltseigener und anstaltsübergreifender geschlossener Systeme werden nach meinem Kenntnisstand KI-Werkzeuge sowohl in redaktionellen Workflows als auch in Produktion, und Verwaltung eingesetzt. In der ARD und den einzelnen Häusern wurden bestehende Netzwerke und Koordinierungsstrukturen, darunter KI-Räte, KI-Boards, das ARD-KI-Netzwerk und andere interne Austauschformate und gemeinschaftliche Projekte weiter ausgebaut. Diese Schnittstellen sollen Informationen mit redaktionellem, juristischem und technischem Charakter bündeln und gegenseitig für die Weiterentwicklung von KI-Know-how auf Basis von Rechts- und IT-Sicherheit sorgen. Die technische Entwicklung findet nun zunehmend unter geregelten organisatorischen Rahmenbedingungen statt.

Gerade für journalistische Arbeitsprozesse gewinnen KI-basierte Assistenzsysteme an Bedeutung, etwa bei Transkriptionen, Übersetzungen, Zusammenfassungen, Rechercheunterstützung oder Bild- und Audiobearbeitung. Vor diesem Hintergrund werden in den Rundfunkanstalten verschiedene KI-Anwendungen erprobt und ihre Einsatzmöglichkeiten für unterschiedliche Zwecke getestet. Dies erfolgt im Rahmen von Pilotprojekten oder Testphasen und dient der Bewertung von Nutzen, Risiken und datenschutzrechtlicher Konformität der jeweiligen Anwendungen.

Zwar eröffnen diese Anwendungen erhebliche Effizienzgewinne, doch müssen sie datenschutzgerecht eingesetzt werden. Dies betrifft insbesondere die Frage, ob personenbezogene Daten in externe Cloud-Dienste eingegeben werden dürfen, wie Geheimhaltungsinteressen geschützt werden und wie verhindert wird, dass KI-Systeme personenbezogene Inhalte unkontrolliert weiterverarbeiten oder reproduzieren. Auch die Gefahr fehlerhafter oder verzerrter Ergebnisse bleibt im redaktionellen Umfeld ein zentrales Risiko, da journalistische Inhalte hohe Anforderungen an Richtigkeit und Glaubwürdigkeit erfüllen müssen.

Relevant war ein einheitliches Tätigwerden der Anstalten gegenüber Meta, denn seit dem 27.05.2025 nutzt das US-Technologieunternehmen auch die öffentlichen Inhalte, die Nutzerinnen und Nutzer auf Facebook, Instagram und WhatsApp veröffentlichen – etwa Fotos, Videos und andere Beiträge, jedoch keine privaten Nachrichten – zum Training eigener KI-Anwendungen. Hierzu wurden die Nutzungsbedingungen entsprechend angepasst. Unternehmen wie auch Privatpersonen

konnten dieser Form der Datenverarbeitung bis zum Stichtag widersprechen. Meines Wissens haben alle Rundfunkanstalten von diesem Recht Gebrauch gemacht und für ihre jeweiligen Social-Media-Konten einen Widerspruch erklärt, um zu verhindern, dass ihre veröffentlichten Inhalte für KI-Trainingszwecke herangezogen werden. Dies ist nicht nur aus datenschutzrechtlichen Gründen sinnvoll, sondern auch im Hinblick auf die Wahrung der redaktionellen Integrität und Kontrolle über eigene Inhalte.

Um den datenschutzrechtlichen Herausforderungen angemessen zu begegnen, hat die RDSK die Orientierungshilfe zum datenschutzkonformen Einsatz von KI im öffentlich-rechtlichen Rundfunk, zuletzt in der Version 2.1 im September 2024[11], veröffentlicht. Entsprechend den rechtlichen und technischen Entwicklungen und auch unter Berücksichtigung der praktischen Erfahrungen aus der Umsetzung in den Rundfunkanstalten wird diese Orientierungshilfe zukünftig weiter durch meine Behörde aktualisiert und angepasst werden.

Es bleibt festzuhalten, dass sowohl die KI-Regulierung als auch die praktische Nutzung von KI-Systemen im Rundfunkumfeld dynamische Entwicklungen durchlaufen. Die Herausforderungen betreffen nicht nur die technische Gestaltung der Systeme, sondern auch rechtliche und organisatorische Rahmenbedingungen – etwa Fragen der Verantwortlichkeit, der Rechtsgrundlagen, der Betroffenenrechte oder der Datenminimierung. Als Rundfunkdatenschutzbeauftragter werde ich diese Entwicklungen auch im kommenden Jahr eng begleiten. In Ansehung der begrenzten Ressourcen ist es nicht möglich, die eingesetzten Systeme im Einzelnen in den Blick zu nehmen. Die Aufgabe der Aufsichtsbehörde besteht darin, die Rahmenbedingungen zu verdeutlichen, auf Risiken hinzuweisen und Handlungsmöglichkeiten zu eröffnen.

6.9 Medienprivileg

Das Medienprivileg beschreibt eine bereichsspezifische Ausnahme, durch die die Medien von den allgemeinen datenschutzrechtlichen Vorgaben weitestgehend ausgenommen werden. Das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) tritt im journalistischen Kontext in den Hintergrund, während das öffentliche Informationsinteresse sowie die Presse- und Rundfunkfreiheit (Art. 5 GG) und damit das Interesse an der Veröffentlichung in den Vordergrund treten und insoweit privilegiert sind.

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

6.9.1 Rechtsgrundlagen und Anwendbarkeit des Medienprivilegs

Die §§ 12 Abs. 1 und 23 Abs. 1 Medienstaatsvertrag (MStV) bestimmen im Rahmen der Öffnungsklausel des Art. 85 Abs. 1 DSGVO, welche datenschutzrechtlichen Vorgaben der DSGVO für die journalistische Datenverarbeitung gelten. Art. 85 Abs. 2 DSGVO nennt bereits jene Bereiche der Verordnung, bei denen die Mitgliedstaaten Ausnahmen oder Abweichungen vorsehen sollen — diese finden sich in den genannten Vorschriften des MStV wieder.

Die DSGVO ist damit für journalistische Tätigkeiten weitgehend nicht anwendbar. Vollständig bestehen bleibt jedoch das Datengeheimnis: Personenbezogene Daten, die zu journalistischen Zwecken erhoben wurden, dürfen nicht für andere Zwecke genutzt werden. Zudem müssen die Integrität und Vertraulichkeit der Daten jederzeit sichergestellt sein.

Ob das Medienprivileg greift, hängt entscheidend davon ab, ob die jeweilige Datenverarbeitung „journalistischen Zwecken“ dient. Nach der Rechtsprechung des EuGH (Urt. v. 14.02.2019 – C-345/17 – Buivids) liegt ein journalistischer Zweck vor, wenn Informationen, Meinungen oder Ideen öffentlich verbreitet werden und damit zur öffentlichen Meinungsbildung beitragen — unabhängig vom eingesetzten Medium. Nach dem BGH (Urt. v. 12.12.2021 – VI ZR 488/19) ist zudem ein Mindestmaß eigener inhaltlicher Aufbereitung erforderlich. Damit können nicht nur klassische Medienunternehmen oder Rundfunkanstalten, sondern auch einzelne Bloggerinnen und Blogger sowie Betreiberinnen und Betreiber von Social-Media-Kanälen unter das Medienprivileg fallen.

Nicht als journalistisch gelten dagegen Tätigkeiten wie die Verarbeitung von Daten für den Rundfunkbeitragseinzug, die Gewinnung von Abonnentinnen und Abonnenten, die kommerzielle Weitergabe von Daten — beispielsweise für Werbezwecke — oder die Nutzung durch Suchmaschinen. Sobald eine Verarbeitung nicht dem journalistischen Bereich zuzuordnen ist, bedarf es einer Rechtsgrundlage nach Art. 6 DSGVO.

Für die redaktionelle und journalistische Datenverarbeitung innerhalb der Rundfunkanstalten findet somit das Medienprivileg Anwendung (siehe auch die Erläuterungen zur im Berichtsjahr durchgeführten Befragung zum Redaktionsdatenschutz, Kapitel 6.1.2). Viele Beschwerden, die etwa die fehlende Einwilligung einer in Beiträgen erkennbaren Person beanstanden, sind daher unter Hinweis auf das Medienprivileg zu beantworten. Unberührt davon bleibt die persönlichkeitsrechtliche Bewertung, die jedoch nicht in die Zuständigkeit der Datenschutzaufsichtsbehörde fällt. Zugleich existieren naturgemäß Grenzbereiche, die zwar Berührungspunkte zur journalistischen Tätigkeit haben, deren Schwerpunkt aber nicht journalistischer Natur ist. Bereits in den Tätigkeitsberichten 2023 (Kapitel 6.3.2 ff.) und 2024

(Kapitel 6.7.2 ff.) wurden solche Bereiche dargestellt, die im Rundfunkdatenschutz von Bedeutung waren.

6.9.2 Was erreichte uns zum Medienprivileg?

Wie bereits dargestellt (siehe Kapitel 6.1.2) treffen den Rundfunkdatenschutzbeauftragten im Rahmen des Redaktionsdatenschutzes eingeschränkte und subsidiäre Pflichten, wie sie in den §§ 12 und 23 des Medienstaatsvertrages niedergelegt sind. Dennoch muss ich mich mit den Beschwerden, die uns im redaktionellen Kontext erreichen, auseinandersetzen und diese an die entsprechenden Kanäle weiterleiten und gleichzeitig die Beschwerdeführenden darüber informieren, warum sie mit ihrer Beschwerde nicht an der richtigen Adresse sind. Insbesondere ist darauf hinzuweisen, dass – auch wenn Datenschutz nicht einschlägig ist – die Anstalten nur im Rahmen der gesetzlichen Regelungen des Persönlichkeitsrechts und des Grundrechtsschutzes frei darin sind, auch identifizierend über Personen zu berichten.

Im Berichtsjahr erreichten meine Behörde zwölf solcher Beschwerden. Gegenstand waren z. B. die Sichtbarkeit von Kfz-Kennzeichen bei einem Bericht über einen Pfingststau, das Zeigen eines Schreibens im Rahmen des Sommerinterviews, in dem personenbezogene Daten erkennbar waren oder die Sichtbarkeit des Namens und Geburtsdatums eines Interviewpartners, der eigentlich anonym bleiben sollte. Ebenso erreichte uns die Beschwerde einer Kommune, dass Wahlhelfer bei einer Kommunalwahl gefilmt worden seien. Inhaltliche Beschwerden zum ZDF Magazin Royal wurden ebenfalls vorgetragen und allgemeine Anmerkungen zu der Qualität des öffentlich-rechtlichen Rundfunks im Kontext der journalistischen Sorgfaltspflicht und journalistischer Standards.

Ich halte es nach wie vor für richtig, dass der Datenschutz keinen Einfluss auf die journalistische Berichterstattung haben darf. Richtig finde ich es aber ebenso, dass die Grenzen der Persönlichkeitsrechte stets gewahrt werden müssen. Daher bemühe ich mich, die Beschwerden an die richtige Stelle weiterzuleiten bzw. ausführlich darüber aufzuklären, dass zwar auf die Unterstützung des Rundfunkdatenschutzbeauftragten in den konkreten Fällen verzichtet werden muss, der Berichterstattung dennoch juristische Grenzen gesetzt sind.

6.9.3 Auskunftsanspruch und Medienprivileg

Eine in der Tat bemerkenswerte Beschwerde erreichte mich im Berichtsjahr, die eine Abgrenzung zwischen Datenschutzrecht und dem Medienprivileg erforderlich machte.

Hintergrund war eine Auseinandersetzung im Rahmen einer Technikprobe im Vorfeld einer Aufzeichnung, in deren Folge es zu einer Beleidigung gekommen sein soll. Die betroffene Landesrundfunkanstalt hat für die interne Aufarbeitung des in Raum stehenden Vorwurfs eine Untersuchung durch eine Anwaltskanzlei beauftragt, im Zuge derer Interviews mit der betroffenen Person und weiteren Mitarbeiterinnen und Mitarbeitern der entsprechenden Fernsehproduktion geführt wurden. Die Ergebnisse der Untersuchung der Kanzlei wurden in einem ausführlichen Untersuchungsbericht dargelegt.

Gegenstand der Beschwerde war ein von der Rundfunkanstalt abgelehnter Auskunftsanspruch, der die Herausgabe sämtlicher personenbezogener Daten und insbesondere die Übergabe des Untersuchungsberichtes der beauftragten Kanzlei beinhaltete.

Der Anspruch wurde zunächst auf § 23 Abs. 2 Medienstaatsvertrag gestützt, wonach die betroffene Person von einem Anbieter von Telemedien, der personenbezogene Daten zu journalistischen Zwecken gespeichert, verändert, übermittelt, gesperrt oder gelöscht hat und dadurch die betroffene Person in ihrem Persönlichkeitsrecht beeinträchtigt wird, Auskunft über die zugrunde liegenden zu ihrer Person gespeicherten Daten verlangen kann. Anspruchsvoraussetzung ist also, dass eine Persönlichkeitsrechtsverletzung oder -beeinträchtigung, verursacht durch einen Telemedienanbieter, vorliegt.

Es wurde vorgetragen, dass die hier betroffene Rundfunkanstalt im Rahmen der Berichterstattung auf ihrer Website und damit als Telemedienanbieter Schilderungen der Beschwerdeführerin in Bezug auf den angegriffenen Vorfall als unzutreffend dargestellt habe. Dies sei eine Beeinträchtigung ihres öffentlichen Ansehens und ihrer Glaubwürdigkeit und mithin als Persönlichkeitsrechtsverletzung einzuordnen.

Grundsätzlich ist die Feststellung einer solchen Persönlichkeitsrechtsverletzung nicht vom Zuständigkeitsbereich des Rundfunkdatenschutzbeauftragten umfasst. Ob die Recherche oder Veröffentlichung eines journalistischen Beitrages Persönlichkeitsrechte verletzt, hat nicht die Datenschutzaufsicht, sondern der für die Berichterstattung Verantwortliche selbst zu beantworten (siehe dazu auch Kapitel 2.3).

Im Zuge der Auseinandersetzung wurde eine solche Persönlichkeitsrechtsverletzung durch die Rundfunkanstalt weder festgestellt noch eingeräumt. Wird dies nicht von der Rundfunkanstalt selbst festgestellt, bedarf es einer gerichtlichen Feststellung. Eine eigene Überprüfung eines äußerungsrechtlichen Sachverhalts steht der Datenschutzaufsicht mangels eines datenschutzrechtlichen Anknüpfungspunktes demgegenüber nicht zu. Ansonsten müsse sich die Aufsichtszuständigkeit des Rundfunkdatenschutzbeauftragten auch auf die Beurteilung von

Ansprüchen aus dem Äußerungsrecht beziehen, was nicht der Fall ist. Im Ergebnis war also der Auskunftsanspruch nicht auf § 23 Abs. 2 MStV zu stützen.

Auch ein Auskunftsanspruch nach Art. 15 Abs. 1, 3 DSGVO war nicht begründet, da sich nach meiner Einschätzung das Auskunftsbegehren auf journalistische und mithin medienprivilegierte Daten bezogen hat.

Zunächst war die Frage zu beantworten, ob Video- und Tonaufnahmen des streitgegenständlichen Gesprächs auskunftsfähig sind. Seitens der Beschwerdeführerin wurde vorgetragen, das Gespräch habe nicht im Rahmen des zur Veröffentlichung geführten Interviews, sondern im Rahmen einer Technikprobe stattgefunden. Die Speicherung diesbezüglicher Aufnahmen habe daher nicht journalistischen Zwecken gedient.

Die weite Ausdehnung des Begriffs Journalismus gebietet es indes, keine Tatbestandsbegrenzungen auf mehr oder weniger professionalisierte journalistische Tätigkeiten vorzunehmen. Die datenschutzrechtliche Freistellung darf nicht von der Einhaltung von journalistischen Sorgfaltsstandards im Einzelfall abhängig gemacht werden. Erfasst sein muss nach meiner Überzeugung jede Datenverarbeitung, die für die Erfüllung des journalistischen Zwecks erforderlich ist. Die dafür notwendigen Tätigkeiten sind weit zu interpretieren, auch und vor allem im Lichte der in Erwägungsgrund 153 zur DSGVO geforderten weiten Auslegung der journalistischen Freiheitsrechte. Der vorliegende enge sachliche, zeitliche und personelle Zusammenhang mit dem geführten Interview, lässt keine andere Bewertung zu, als auch die im Rahmen der Technikprobe gemachten Aufnahmen dem journalistischen Bereich zuzuordnen.

Schwieriger zu beantworten war die Frage, ob der Untersuchungsbericht der Kanzlei zum streitgegenständlichen Fall ebenfalls dem Medienprivileg unterfällt. Die Rundfunkanstalt hat sich dahingehend eingelassen, dass der Untersuchungsbericht selbst nicht primär journalistischen Zwecken diente, der Kontext aber eine öffentlich ausgetragene Auseinandersetzung über die Vorwürfe sei. Da diese Äußerungen in einem Vorbereitungsgespräch zu einer Sendung getätigt worden seien, sei die Anstalt in ihrem gesetzlichen Auftrag berührt. Aspekte der Programmgestaltung seien vordringlich und entscheidend, wenn etwa Mitarbeiterinnen und Mitarbeiter aufgrund solcherlei Vorwürfe nicht mehr programmgestaltend arbeiten dürfen.

Zu den medienprivilegierten Tätigkeiten zählen zweifellos die Kerntätigkeit journalistischen Arbeitens, aber auch solche Verwaltungs- und Hilfstätigkeiten, die ein journalistisches Arbeiten überhaupt erst ermöglichen, indem sie die notwendigen administrativen Voraussetzungen für ein freies journalistisches Arbeiten schaffen. Wichtig ist, dass ein innerer Zusammenhang zur journalistischen Kerntätigkeit besteht. Die Abgrenzung zu Verwaltungstätigkeiten und

journalistischer Tätigkeit ist oftmals schwer zu treffen. Man kann sich am BGH orientieren, der festgehalten hat, dass Daten „dann zu journalistisch-redaktionellen Zwecken verarbeitet werden, wenn die Zielrichtung einer Veröffentlichung für einen bestimmten Personenkreis besteht“ (Urteil vom 15.12.2009 – VI ZR 227/08 Rn. 31).

Ich habe unter Berücksichtigung der anzuwendenden weiten Auslegung die Auffassung vertreten, dass es genügt, wenn die Datenverarbeitung insgesamt und unter einem breiten Blickwinkel diesen Anforderungen entspricht. Der Untersuchungsbericht selbst war Gegenstand der Berichterstattung auch von der betroffenen Rundfunkanstalt. Der Kontext war die Frage nach journalistischen Verfehlungen, Standards des öffentlich-rechtlichen Rundfunks und der erkennbare Wunsch, die Umstände des innerhalb einer journalistischen Produktion geschehenen Vorfalls aufzuarbeiten. Dem steht auch nicht entgegen, dass der Untersuchungsbericht nicht für Zwecke einer Berichterstattung angefertigt wurde, sondern erst später zum Gegenstand einer solchen wurde. Der umfassende Schutzbereich der freien journalistischen Berichterstattung erfordert es, hier weder zeitliche noch sachliche Grenzen zu setzen. Auch eine Datenverarbeitung, die erst im Laufe der Entwicklung journalistisches Profil gewinnt und entsprechenden Zwecken zu dienen geeignet ist, muss unter das Medienprivileg fallen, da sonst eine schwer begründbare Grenze gesetzt würde, die der grundrechtlich geschützten Rundfunkfreiheit entgegenstünde.

Es bleibt festzuhalten, dass dieser Fall eindeutig den Grenzbereich des Medienprivilegs betrifft, da nur eine sehr weite Auslegung dieses Ergebnis stützt. Die Gesamtumstände haben mich bewogen, hier der Rundfunk- und Medienfreiheit ein höheres Gewicht einzuräumen.

6.9.4 Unberechtigte Weitergabe von personenbezogenen Daten

Im Sommer des Berichtsjahres erreichte mich eine Beschwerde, dass eine Anfrage zu einer kommunalen Veranstaltung durch die berichtende Rundfunkanstalt direkt an den Veranstalter weitergegeben worden sei. In der weitergeleiteten E-Mail befanden sich auch personenbezogene Daten des Beschwerdeführers, der sich einerseits in seinen Persönlichkeitsrechten verletzt sah und andererseits ein Konfliktpotential mit der Kommune skizzierte, das in Ansehung des an sich harmlosen Inhalts wenig nachvollziehbar schien.

Dessen ungeachtet stellte sich diese Weiterleitung der E-Mail als eine Verletzung des Datenschutzes heraus. Bekanntermaßen dürfen Daten zu journalistischen Zwecken verarbeitet werden, ohne dass es einer speziellen Rechtsgrundlage dafür bedarf. Das Medienprivileg stellt den Journalismus, wie bereits in den Kapiteln zuvor erläutert, von den Anforderungen des Datenschutzrechts weitgehend frei. Eine medienprivilegierte Datenverarbeitung liegt dann vor, wenn sie das Ziel verfolgt, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten. Ein weites

Begriffsverständnis schließt auch solche Tätigkeiten ein, die nur im weitesten Sinne der journalistischen Arbeit zuzuordnen sind, dazu gehören gewiss auch die Beantwortung von Zuschaueranfragen oder allgemein der Kontakt zu Nutzerinnen und Nutzern, soweit es sich um den Austausch zu journalistischen Inhalten handelt.

Die Weiterleitung der E-Mail mit den personenbezogenen Daten an den Veranstalter hatte aber nicht diese Zielrichtung, man wollte dem Beschwerdeführer offensichtlich einfach einen Gefallen tun und ihm eine weitere Kontaktaufnahme mit dem Veranstalter abnehmen bzw. die Kontaktaufnahme erleichtern. Die Journalistin hatte nach meiner Kenntnis die Anfrage deshalb an den Veranstalter weitergeleitet, da sie annahm, dass der Beschwerdeführer die Kontaktaufnahme ohnehin plante. Die Weitergabe der Kontaktdaten hatte demnach nicht das Ziel, zur öffentlichen Meinungsbildung beizutragen. Es handelte sich somit um keine medienprivilegierte Datenverarbeitung, sodass die DSGVO vollständig Anwendung fand.

Unabhängig davon, ob die Annahme der Journalistin richtig war oder nicht, fehlt es hier im Ergebnis an einer wirksamen Einwilligung oder einer sonstigen Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO. Die Rundfunkanstalt habe ich daher angewiesen, künftig bei der Beantwortung von Anfragen von Zuschauerinnen und Zuschauern sorgfältiger vorzugehen und insbesondere darauf zu achten, dass die Daten allein im journalistischen Kontext verbleiben. Es ist also zu bewerten, ob in diesem Zusammenhang etwaige personenbezogene Daten noch im Rahmen von journalistischen Zwecken ausgetauscht werden sollen, oder ob eine Einwilligung erforderlich ist. Im Zweifel ist zu einer vorherigen Einwilligung zu raten, um Datenschutzverstöße auszuschließen.

Der hier geschilderte Fall ist im Ergebnis als wenig kritisch einzuordnen, wenngleich der Beschwerdeführer massive persönliche Folgen befürchtet hatte. Diese waren aber nicht nachvollziehbar und kaum als direkte Folge der Offenlegung des Inhalts der Mail und der personenbezogenen Daten anzunehmen. Dennoch zeigt dieser Fall anschaulich, dass Journalistinnen und Journalisten besonders sorgfältig mit im journalistischen Kontext verarbeiteten personenbezogenen Daten umgehen müssen und stets dafür sensibilisiert werden sollten, dass die journalistische Zweckbindung eingehalten werden muss.

6.9.5 Speicherung und Verarbeitung von Interviewdaten bei Straßenumfragen

Zu den Aufgaben der Datenschutzaufsicht gehört auch die Beratung der einzelnen Landesrundfunkanstalten. Im Berichtsjahr erreichte mich die Frage eines Personalrates, inwieweit eine von der Rundfunkanstalt veranlasste Regelung zulässig sei. Nach dieser Regel sind Reporterinnen und Reporter der Rundfunkanstalt verpflichtet, Menschen, die zu ihrer Meinung hinsichtlich eines Themas befragt werden, grundsätzlich auch nach deren Adresse und

Parteizugehörigkeit zu fragen, und ebenso dazu, ob sie schon einmal bei einer Landesrundfunkanstalt des ARD-Verbundes beschäftigt waren.

Ich habe zunächst das Medienprivileg ausführlich erläutert und in diesem Zusammenhang dargestellt, dass auch die hier in Rede stehende Datenerhebung vom Medienprivileg gedeckt ist. Denn es handelt sich dabei um journalistische Datenverarbeitungen im Rahmen von Recherchen. Kein Problem konnte ich ebenso darin erkennen, dass diese Daten bis zu vier Wochen gespeichert werden, auch dies ist vom Medienprivileg gedeckt. Hingewiesen habe ich aber darauf, dass die Speicherung in der Zentralen Austauschplattform in Hinblick auf Datensicherheit geprüft werden müsse, insbesondere habe ich darauf aufmerksam gemacht, dass die Zugriffe auf diese Plattform auf das Notwendigste und insbesondere auf journalistische Zwecke beschränkt sein müssen.

Solche Anfragen zeigen, dass offensichtlich Unsicherheiten im Umgang mit journalistisch veranlasster Datenverarbeitung bestehen. Dies habe ich auch im Rahmen des Audits zum Redaktionsdatenschutz (siehe Kapitel 6.1.2) festgestellt. Positiv hervorzuheben ist jedoch das vorhandene Problembewusstsein sowie die frühzeitige Einbindung der Aufsicht, die es ermöglicht hat, den Sachverhalt schnell und unbürokratisch zu klären.

6.10 Übertragung zusätzlicher Aufgaben an den Datenschutzbeauftragten

Um Rat ersucht wurde in der Frage, inwieweit interne Datenschutzbeauftragte im Rahmen zusätzlicher Pflichten und Aufgaben gemäß Art. 38 Abs. 6 DSGVO auch damit betraut werden können, Auskunftsersuchen und weitere Betroffenenanfragen entgegenzunehmen und sie zur Beantwortung an die entsprechenden Stellen zu verteilen. Ebenso müssen die gesammelten Antworten sodann an die betroffene Person versandt werden.

Die DSGVO gestattet gemäß Art. 38 Abs. 6, dass betriebliche Datenschutzbeauftragte auch andere Aufgaben und Pflichten wahrnehmen können. Es ist sicherzustellen, dass eine Übertragung dieser Aufgaben nicht zu einem Interessenskonflikt führt. Dies ist dann anzunehmen, wenn zumindest die Gefahr besteht, dass die Datenschutzbeauftragten durch dienstliche oder wirtschaftliche Interessen in der objektiven Wahrnehmung ihrer gesetzlichen Aufgaben und Pflichten eingeschränkt sind. Sie dürfen daher nicht gleichzeitig Tätigkeiten wahrnehmen, die sie dazu veranlassen würden, die Zwecke und Mittel der Verarbeitung personenbezogener Daten bei der verantwortlichen Stelle festzulegen.

Leitbild der Stellung des betrieblichen Datenschutzbeauftragten ist seine Unabhängigkeit bei der Erfüllung seiner Aufgaben. Diesen kann er nur nachkommen, wenn er nicht in die Pflicht genommen

wird, über Zwecke und Mittel der Verarbeitung zu entscheiden und sich damit dem Konflikt ausgesetzt sieht, die von ihm verantwortete Datenverarbeitung in Personalunion ebenso zu überwachen.

Der von mir zu bewertende Fall, also der Organisation der Beantwortung und anschließenden Versendung von Auskunftsersuchen durch die betrieblichen Datenschutzbeauftragten, ist mit Art. 15 DSGVO und dem skizzierten Trennungsgebot zu vereinbaren. Entscheidend ist, dass die Übertragung der anderen Pflichten so gestaltet ist, dass der betriebliche Datenschutzbeauftragte diese Aufgaben nicht in seiner Funktion als Datenschutzbeauftragter wahrnimmt und ebenso seine unabhängige Amtsführung nicht tangiert wird. Die hier zu betrachtende Aufgabenübertragung kann deswegen möglich sein, weil der Datenschutzbeauftragte bei Sichtung und Versendung der Informationen, die im Rahmen von Auskunftsersuchen an die betroffene Person ausgereicht werden müssen, die Rechtmäßigkeit und Vollständigkeit der Auskünfte in seiner Rolle als Datenschutzbeauftragter gleichsam überwachen und kontrollieren kann. Da dies ohnehin seine Aufgabe ist, erzeugt dies keinen grundsätzlichen Interessenskonflikt.

In jedem Fall ist bei zusätzlichen Aufgabenübertragungen jedoch immer Vorsicht und Präzision angebracht, damit das Leitbild des unabhängigen internen Datenschutzbeauftragten nicht beeinträchtigt wird.

6.11 Private Nutzung dienstlicher Kommunikationswege (Mitarbeiterexzess)

Im Berichtsjahr erreichte mich eine Beschwerde des Inhalts, dass eine Mitarbeiterin Schriftverkehr im Rahmen eines privaten Schadensfalls und im Zusammenhang mit einer diesbezüglichen juristischen Auseinandersetzung über ihren dienstlichen E-Mail-Account der Rundfunkanstalt abgewickelt und diesen damit für private Zwecke benutzt hat. Es wurde gerügt, dass in dieser Kommunikation seitens der Mitarbeiterin persönliche Daten einer in den privaten Konflikt involvierten Person angeführt worden seien.

Es stellten sich dabei folgende Fragen: Wie ist die Verantwortung im datenschutzrechtlichen Sinne zu beurteilen, wenn Mitarbeitende der Rundfunkanstalten private Angelegenheiten über dienstliche Accounts regeln und damit ggf. den Eindruck erwecken, als Vertreter dieser Anstalt aufzutreten? Und inwieweit ist die Rundfunkanstalt für die Verarbeitung dieser Daten verantwortlich, allein deshalb, weil die Daten in den Systemen der Anstalt vorhanden sind?

In diesem Fall hat die Stellungnahme des zuständigen internen Datenschutzbeauftragten ergeben, dass die Kontaktaufnahme und Kommunikation über den dienstlichen E-Mail-Account

ausschließlich dem privaten Kontext zuzuordnen war und damit ein sogenannter Mitarbeiterexzess vorlag. Die Person, die den E-Mailaccount für persönliche und damit außerdienstliche Zwecke nutzt, ist dann als verantwortlich im Sinne des Art. 4 Abs. 1 DSGVO anzusehen. Die Verantwortung der Rundfunkanstalt scheidet insoweit aus, wenn die private Nutzung der Accounts untersagt ist. Ebenso muss ein dienstlicher Bezug oder die Zurechnung zum Verantwortungsbereich der Anstalt ausgeschlossen sein, wodurch Ansprüche gegen die Anstalt nach Art. 15, 17 oder 82 DSGVO ausgeschlossen sind.

Im vorliegenden Fall sind die privaten E-Mails aus den Systemen der Anstalt entfernt worden, damit wurde eine saubere Trennung auch im technisch-organisatorischen Bereich vollzogen. Die Rundfunkanstalt kann nicht dulden, dass private Daten in ihren Systemen gespeichert werden, die keinen dienstlichen Bezug haben.

Der Beschwerdeführer wurde insoweit über die rechtlichen und tatsächlichen Umstände informiert, und der Fall konnte damit abgeschlossen werden.

6.12 Internationale Zusammenarbeit zwischen Aufsichtsbehörden

Von einer Landesrundfunkanstalt erreichte mich die Anfrage eines Journalisten, der mir eindringlich sein Problem schilderte. Er werde von einer Person aus Israel mit Hass-Mails geflutet, die abgesehen von den beleidigenden Inhalten auch an einen immens großen Verteiler gerichtet seien, sodass die personenbezogenen Daten des Journalisten in diesem Kontext weit verbreitet würden. Der Journalist fragte mich, inwieweit internationale Kontakte auch zu den israelischen Datenschutzbehörden bestünden bzw. die Zusammenarbeit erfolgen könne.

Ich habe darauf hingewiesen, dass allein im europäischen Rechtsraum die Verpflichtung und auch die Möglichkeit besteht, dass sich Betroffene mit Beschwerden immer an die Datenschutzbehörde an ihrem Wohnsitz wenden können, die sich sodann mit der Frage beschäftigen und ggf. auch andere europäische Aufsichtsbehörden mit einbeziehen muss. Eine Zusammenarbeit mit den israelischen Datenschutzbehörden besteht in dieser Hinsicht jedoch nicht, sodass ich in einem ausführlichen Gespräch mit dem betroffenen Journalisten lediglich auf die Möglichkeit verweisen konnte, sich mit seinem Anliegen direkt an die israelischen Aufsichtsbehörden zu wenden; einen Kontakt im Rahmen eines Amtshilfeverfahrens konnte ich jedoch nicht herstellen.

7 Datenschutz in den Rundfunkanstalten

Dieses Kapitel stützt sich insbesondere auf die Erkenntnisse aus den vierteljährlichen Jour fixes mit den internen Datenschutzbeauftragten der Rundfunkanstalten und gibt einen Einblick in die Datenschutzorganisation.

Den 2024 ins Leben gerufenen Jour fixe mit den jeweiligen Datenschutzbeauftragten (und optional deren Stellvertretungen oder direkten Assistenzen) der beaufsichtigten Rundfunkanstalten und des Beitragsservices habe ich 2025 weitergeführt. Insgesamt haben mein Team und ich so in jedem Quartal 10 Jour fixes durchgeführt und damit einen Überblick über aktuelle Datenschutzthemen erhalten. Gleichzeitig habe ich verfolgt und eingefordert, ob und dass sich die Organisation des Datenschutzes hin zu einem lebendigen Datenschutzmanagementsystem (DSMS) weiterentwickelt. Die Verantwortlichen sind aufgerufen, rechtliche, technische und organisatorische Anforderungen integriert zu steuern und dauerhaft zu überwachen.

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

7.1 Einführung bzw. Weiterentwicklung eines Datenschutzmanagementsystems

Datenschutz ist für die Verantwortlichen eine Organisationsaufgabe, er funktioniert umso besser, je klarer die Strukturen definiert, überwacht und kontinuierlich verbessert werden.

In meinen Gesprächen zum Stand der Einführung eines Datenschutzmanagementsystems (DSMS) bestand grundsätzlich Einvernehmen, dass bereits bestehende Vorgaben zu einem DSMS fortzuentwickeln sind, soweit ein solches nicht bereits implementiert ist. Das für das Berichtsjahr 2025 gesetzte Ziel der Einführung eines Datenschutzmanagementsystems aller durch mich beaufsichtigten Rundfunkanstalten wurde von einigen Rundfunkanstalten erreicht, während andere das Ziel auf das Jahr 2026 verschieben mussten. Beispielsweise, weil die Aufstellung eines Projektteams länger als gedacht gedauert hat oder andere Themen in den Rundfunkanstalten priorisiert werden mussten.

Weil sich anhand der dargestellten Regelungen und Informationen zum Datenschutzmanagement in den Gesprächen zeigte, dass unterschiedliche Auffassungen hinsichtlich Anforderungen, Inhalt und Umfang eines DSMS vorlagen, war dies Anlass für mich, unterstützend tätig zu werden.

Erarbeitet und im Dezember 2025 den Datenschutzbeauftragten der Rundfunkanstalten zur Verfügung gestellt wurde die Handreichung „Datenschutzmanagement-Check“, die die Rundfunkanstalten dabei unterstützen soll, den aktuellen Stand des Datenschutzmanagement(system)s zu erheben und weiterzuentwickeln (vergleiche hierzu auch Kapitel 7).

Die Handreichung umfasst einführende Erläuterungen sowie drei Checklisten, die sich in einer zugehörigen Excel-Tabelle wiederfinden und eine nachvollziehbare Dokumentation von Entwicklungsständen ermöglichen:

- Datenschutzmanagement: Ausprägung reaktiv bzw. proaktiv
- Datenschutzprozesse: Reifegradeinstufung einzelner Prozesse
- Datenschutzmanagementsystem: Entwicklungsstand der Kernelemente eines DSMS

Der anhand der Checklisten dokumentierte Fortschritt soll durch die Datenschutzbeauftragten im Folgejahr regelmäßig fortgeschrieben werden und die Weiterentwicklung in den Jour fixes beobachtet werden.

7.2 Kennzahlen zu Eingabebearbeitung und Datenschutzvorfällen

In den Jour fixes wurden zugleich statistische Kennzahlen zu Beschwerden, Auskunftsanfragen sowie zu Datenschutzvorfällen thematisiert. Im Berichtsjahr rückte dabei insbesondere die Anzahl nicht meldepflichtiger Datenschutzvorfälle in den Rundfunkanstalten in den Fokus. Sofern über mehrere Quartale hinweg keinerlei Vorfälle mit geringem Risiko ausgewiesen wurden, wurde dies von mir zum Anlass genommen zu verdeutlichen, dass eine fehlende entsprechende Kennzahl sowohl auf sehr gut funktionierende Prozesse als auch auf Defizite in der Erfassung und Bewertung von Vorfällen hindeuten kann (siehe Kapitel 5.2). Vor diesem Hintergrund wurde eine Überprüfung der Wirksamkeit der internen Prozesse angeregt.

Nach meiner Kenntnis ging bei den Rundfunkanstalten über die betrachteten Quartale hinweg eine überschaubare Anzahl von Auskunftsanfragen und Datenschutzbeschwerden ein, die nicht den Beitragsservice betrafen. Zugleich berichteten die Rundfunkanstalten über ein vermehrtes Aufkommen pauschaler Auskunftsanfragen, die über die Plattform *wiple.com* übermittelt wurden. Vor diesem Hintergrund verständigten sich die internen Datenschutzbeauftragten auf ein einheitliches Vorgehen, um das verhältnismäßig hohe Anfrageaufkommen sachgerecht und effizient bewältigen zu können.

7.3 Datenschutzrechtliche Themenschwerpunkte

Um an die „Datenschutzrealität“ der Rundfunkanstalten anknüpfen zu können, ist für mich von Interesse, mit welchen datenschutzrechtlichen Themen oder neuen/sich ändernden Anwendungen die Datenschutzbeauftragten sich schwerpunktmäßig beschäftigt haben. So ergibt sich über das Jahr hinweg ein anschauliches Bild der den Datenschutz betreffenden Arbeitsschwerpunkte. Neben dem Tagesgeschäft lagen im Berichtsjahr beispielsweise auch die Schaffung gemeinschaftlicher Anwendungen der ARD oder der Umgang mit KI im Fokus des Datenschutzes.

8 Datenschutz beim Beitragsservice

Der Beitragsservice von ARD, ZDF und Deutschlandradio verwaltet die Daten der Rundfunkbeitragszahlerinnen und -zahler in einem Rechenzentrum in Köln. Klagen sowie Rechtsangelegenheiten werden dagegen dezentral von den einzelnen Rundfunkanstalten betreut, da der Beitragsservice als nicht rechtsfähige öffentlich-rechtliche Verwaltungsgemeinschaft betrieben wird (vgl. § 10 Abs. 7 RBStV).

Der Rundfunkdatenschutzbeauftragte übernimmt die datenschutzrechtliche Kontrolle über die Verarbeitung der Daten beim Beitragsservice.

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 sachliche, professionelle und kooperative Zusammenarbeit verdient an dieser Stelle besondere Erwähnung.

Stets berichtet die behördliche Datenschutzbeauftragte überdies im AK DSB, ist in die dortigen Diskussionen eingebunden und wirkt an der Lösung von Rechtsfragen mit.

Aufsichtsrechtlich stehe ich und stand 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.

8.1 Fragwürdiger Service für Rundfunkbeitragsangelegenheiten

In meinem Tätigkeitsbericht des Jahres 2024 habe ich unter Ziffer 8.1 über einen Onlineservice berichtet, der kostenpflichtige Dienstleistungen (z. B. Anmeldungen, Adressänderungen, Änderungen der Bankverbindungen) rund um den Rundfunkbeitrag anbietet. Diese kann man allerdings kostenlos auch selbst auf den Seiten des Beitragsservice erledigen (www.rundfunkbeitrag.de).

Im Jahr 2025 hat sich dieses Phänomen verstetigt. Unter einer anderen Adresse hat ein privater Anbieter ebenso kostenpflichtige Dienstleistungen angeboten, die beim Beitragsservice unentgeltlich zu erhalten sind – also die gleiche Geschäftsidee. Unabhängig davon, dass diese Dienstleistung aus Sicht der ebenfalls mit dem Thema befassten Verbraucherschützer rechtswidrig sein dürfte, kam es im Berichtsjahr immer wieder vor, dass falsche Daten über diesen Dienstleister zum Beitragsservice gemeldet wurden oder es zu einer Vermischung von Daten kam.

Diese Datenschutzverstöße wurden mir vom Beitragsservice angezeigt, als Aufsicht bin ich aber für diesen Anbieter nicht zuständig. Das Impressum war insofern bemerkenswert, als dass sich dieser Anbieter in Dubai befindet. Einen Vertreter des Unternehmens in der EU war nicht festzustellen.

Ich hatte mich daher entschlossen, den Landesdatenschutzbeauftragten des Landes Rheinland-Pfalz anzusprechen und ihn für das Thema zu sensibilisieren. Verschiedene Anhaltspunkte sprachen für dessen Zuständigkeit.

Der Landesdatenschutzbeauftragte von Rheinland-Pfalz hat mich darauf hingewiesen, dass seiner Behörde bereits mehrere Beschwerden zu der gegenständlichen Website vorliegen. Im Rahmen der Recherche hat sich tatsächlich herausgestellt, dass es sich um dasselbe Unternehmen handelte, welches schon Betreiber der anderen Website mit dem gleichen „Geschäftsmodell“ war. Gegen das Unternehmen wurde 2025 das Insolvenzverfahren eröffnet, sodass die Verwaltungs- und Verfügungsbefugnis über das Vermögen auf den Insolvenzverwalter übergegangen ist. Die Landesdatenschutzbehörde Rheinland-Pfalz ist im Rahmen der Beschwerdeverfahren nun an die Beschwerdeführer und an den Insolvenzverwalter herangetreten. Aktuell ist die Website nach wie vor online, Beschwerden und Meldungen dazu haben mich allerdings nicht mehr erreicht. Zwar kann ich mangels Zuständigkeit nicht tätig werden, das Thema ist jedoch auch aus Rundfunkdatenschutz-Sicht hoch interessant, so dass ich die Entwicklungen weiterverfolgen werde.

8.2 Konzertierte Aktion gegen den Beitragsservice

„Hol dir deine GEZ-Daten – Schadensersatz bis zu 1200 € möglich“. Unter dieser Überschrift hat eine Website eine Aktion gestartet, die leicht erkennbar das ausschließliche Ziel hatte, Schadensersatz zu generieren. Die Website hat ein Muster einer Auskunftsanfrage gemäß Art. 15 DSGVO bereitgestellt, das eine vollständige Kopie aller personenbezogenen Daten gemäß Art. 15 Abs. 3 DSGVO sowie Übermittlung sämtlicher Informationen gemäß Art. 15 Abs. 1 lit. a bis h DSGVO verlangte. Grundsätzlich müssen Auskunftsanfragen innerhalb eines Monats bearbeitet werden. Ist dies nicht der Fall, liegt im Regelfall ein Datenschutzverstoß vor.

Diese Aktion wurde kurz vor Weihnachten 2025 gestartet mit dem erkennbaren Ziel, den Beitragsservice unter Druck zu setzen und verspätete Auskünfte zu generieren - mit dem aus meiner Sicht nicht einlösbaren Versprechen, eine erhebliche Summe an Schadensersatz zu generieren.

Zunächst muss man wissen, dass sich der Auskunftsanspruch gegenüber dem Beitragsservice im Hinblick auf die Daten zum Beitragseinzug allein nach § 11 Abs. 8 des Rundfunkbeitragsstaatsvertrages (RBStV) richtet. Gemäß dieser Vorschrift sind weniger Datenkategorien mitzuteilen und auch eine Kopie der personenbezogenen Daten ist nicht vorgesehen. Beim Beitragsservice ist das Verfahren der Auskunftserteilung automatisiert.

Entscheidend für mich als Aufsichtsbehörde ist jedoch, dass durch die unseriösen Versprechungen uns ein erhebliches Maß an Beschwerden erreicht hat, insbesondere im Hinblick darauf, dass die gemäß § 11 Abs. 8 RBStV erteilte Auskunft nicht als vollständig akzeptiert und als europarechtswidrig kritisiert wurde. Dies hat dazu geführt, dass die Eingaben Anfang des Jahres 2026 sprunghaft angestiegen sind.

Zu prüfen wird noch sein, ob das Urteil des EuGH vom 19.03.2026 und die dortige Entscheidung dazu, wann ein Auskunftsantrag als exzessiv abgelehnt werden kann, auf solcherlei Aktionen Anwendung findet. Der EuGH hat immerhin klargestellt, dass auch ein erstmaliger Antrag exzessiv im Sinne von Art. 12 Abs. 5 DSGVO sein kann und der Nachweis einer missbräuchlichen Verhaltensweise die Gesamtheit der objektiven Umstände zu berücksichtigen hat. Auch muss ein subjektives Element vorliegen, nämlich die Absicht der antragstellenden Person, sich einen Vorteil zu verschaffen, indem sie die Voraussetzungen für diesen Vorteil künstlich herstellt, mithin die Missbrauchsabsicht unterstellt werden kann. Der jeweils Verantwortliche, also die Rundfunkanstalten bzw. der Beitragsservice, tragen dafür die Beweislast. Eine solche konzertierte Aktion, die erkennbar das Ziel verfolgt, den Beitragsservice in eine Schadensersatzsituation zu zwingen, könnte diese Voraussetzungen erfüllen. Im Jahr 2026 werde ich dieses Thema gewiss erneut aufgreifen.

8.3 Sorgt KI für eine Beschwerdeflut?

Die Berliner Datenschutzbeauftragte hat Anfang des Jahres 2026 von einem alarmierenden Anstieg der Eingaben bei ihrer Behörde berichtet (ebenso weitere Aufsichtsbehörden – siehe Vorwort). Sie meint den Hauptgrund für diesen Anstieg gefunden zu haben: Die fortschreitende Digitalisierung und der Einsatz von KI-Chatbots. Sie warnt gleichzeitig davor, dass die Aussagen und vor allem die Einschätzungen der Rechtslage KI-generierter Eingaben oft unvollständig oder schlicht falsch seien. Es sei daher ratsam, die KI-Ergebnisse kritisch zu hinterfragen.

Diese Beobachtung kann ich in meinem Aufsichtsspektrum bestätigen. Die Eingaben auf der einen Seite, aber auch die Reaktionen auf meine Entgegnungen und Erläuterungen der Rechtslage auf der anderen Seite lassen oft vermuten, dass die Eingaben und auch Reaktionen mithilfe von KI erstellt worden sind. Anhaltspunkt dafür ist nach meiner Beobachtung, dass solche Zuschriften ausufernde und verschiedene Rechtsgebiete (insbesondere das Europarecht) streifende Ausführungen enthalten, denen von Seiten meiner Behörde mit den entsprechenden rechtlichen Argumenten begegnet werden muss. So wird insbesondere die Vereinbarkeit des deutschen Rundfunkbeitrags- und Datenschutzrechts mit den unionsrechtlichen Vorgaben infrage gestellt und ebenso die Stellung des unabhängigen Rundfunkdatenschutzbeauftragten. Dies stellt kein grundsätzliches Problem dar, wirkt sich aber auf die Kapazitäten meiner Behörde aus, die bei der Beantwortung solcher Rechtsfragen gefordert ist. Anhand meiner bisherigen Erfahrungen hat sich nämlich herausgestellt, dass die vermutlich von KI-Chatbots angestellten rechtlichen Erwägungen im Ergebnis nicht viel Substanz aufweisen, und dass wesentliche Umstände nicht berücksichtigt werden. Die Spezialmaterie des Rundfunks- und des Rundfunkbeitragsrechtes kann von einer KI offensichtlich (noch) nicht hinreichend bewältigt werden. Ich bin gespannt auf die weiteren Entwicklungen und werde im Bericht über das Jahr 2026 das Thema gewiss erneut aufgreifen.

8.4 Abgrenzung Datenschutzrecht und Beitragsrecht

Ein „Dauerbrenner“ in der aufsichtsrechtlichen Praxis sind Fälle, in denen beitragsrechtliche Fragen streitig sind, die in der vermeintlich engen Verknüpfung mit einer angenommenen Verletzung des Datenschutzrechts dem Rundfunkdatenschutzbeauftragten zur Klärung vorgelegt werden. Beispielhaft sei hier über einen Fall berichtet, in dem eine Person aufgrund ihres Status als Touristin ihre Beitragspflicht anzweifelte. Vorgetragen wurde seitens der Beschwerdeführerin, dass objektive Tatsachen vorlägen, die ihren Status belegten und daher die mit der vom Beitragsservice angenommenen Beitragspflicht zusammenhängende Datenverarbeitung unzulässig und vom Datenschutzbeauftragten zu unterbinden sei.

Im konkreten Fall entwickelte sich ein langer Schriftverkehr, in dem ich zu vermitteln versuchte, dass sich die Beschwerde nicht auf einen datenschutzrechtlich zu bewertenden Sachverhalt bezog, sondern allein auf die Tatsache, ob eine Beitragspflicht bestand. Dies ist nach Rundfunkbeitragsrecht zu beurteilen und insbesondere danach, ob in dem fraglichen Zeitraum die Inhaberschaft an einer Wohnung bestand. Dies bemisst sich insbesondere anhand melderechtlicher Anknüpfungspunkte. Der Beitragsservice hat im Rahmen der von mir eingeforderten Stellungnahme mehrfach mitgeteilt, dass die Einwohnermeldebehörde in dem hier fraglichen Zeitraum mitgeteilt habe, dass die Beschwerdeführerin einwohnermelderechtlich durchgehend mit alleiniger Anschrift in Deutschland gemeldet worden war. Eine Reaktion auf sogenannte Klärungsschreiben, die diesen Umstand verifizieren sollen, sei nicht erfolgt. Damit ist der Beitragsservice grundsätzlich berechtigt, die Person zu einem Beitragskonto anzumelden.

An diesem Beispiel ist erkennbar, dass der Beitragsservice richtig gehandelt und keine Daten unzulässig verarbeitet hat. Streitig ist allein, ob die Informationen, die als Grundlage für die Beitragspflicht dienen, auch den tatsächlichen Umständen entsprechen. Es könnte sich in der Tat um eine fehlerhafte Datenverarbeitung handeln, die allerdings in Ansehung der korrekten Anwendung des Beitragsrechts zunächst unbeachtlich ist. Nur nach Feststellung einer nicht bestehenden Beitragspflicht müssten Daten tatsächlich berichtigt und ggf. gelöscht werden.

Aus Sicht Beschwerde führender Personen verarbeitet der Beitragsservice allerdings unzutreffende und mithin falsche Daten und die Abgrenzung zwischen Beitragsrecht und Datenschutzrecht will ihnen nicht immer einleuchten. Ich habe also in verschiedenen Fällen die nicht einfach zu verstehende Abgrenzung zu erläutern und in möglichst klaren Worten zu vermitteln, erkenne aber an dem teilweise sehr umfangreichen Schriftverkehr, dass es nicht immer gelingt. Dennoch ist es wichtig, den Beschwerdeführenden möglichst ausführlich zu antworten; dieses Thema wird uns in der Aufsichtspraxis auch künftig begleiten.

8.5 Datenübermittlung nach § 11 Abs. 4 Rundfunkbeitragsstaatsvertrag

Der Beitragsservice ist darauf angewiesen, einen vollständigen und korrekten Datenbestand zu haben. Daher sieht der Rundfunkbeitragsstaatsvertrag in § 11 Abs. 5 Rundfunkbeitragsstaatsvertrag (RBStV) eine regelmäßige Datenübermittlung der Meldebehörden an einem bundesweit einheitlichen Stichtag vor. In § 11 Abs. 4 RBStV ist geregelt, dass Meldebehörden unter bestimmten Voraussetzungen Daten übermitteln können, die Rückschlüsse auf die Beitragspflicht zulassen.

Im Berichtsjahr erreichte mich eine Anfrage einer Rechtsanwaltskanzlei, die als externe Datenschutzbeauftragte – ihren eigenen Angaben gemäß – eine Vielzahl von Verwaltungen in

Thüringen betreut. Dort – so die Einlassung der Kanzlei – sei die Abfrage von Meldedaten außerhalb des vierjährigen Zeitraums nach § 11 Abs. 5 RBStV jedoch fraglich, da es an einer entsprechenden Regelung in der Thüringer Meldeverordnung fehle.

In der Tat wird die Auffassung vertreten, dass § 11 Abs. 4 RBStV eine ausreichende Rechtsgrundlage für die Befugnis der Meldebehörden sei, Datenübermittlungen anlassbezogen vorzunehmen. Zumindest für Thüringen gilt jedoch, dass im August 2025 eine Änderung der Meldeverordnung in Kraft getreten ist. Dort wird festgelegt, dass die Meldebehörde dem Mitteldeutschen Rundfunk oder dem Beitragsservice im Fall der Anmeldung, der Abmeldung, einer Namensänderung oder des Todes bestimmte Daten volljähriger Einwohner übermitteln darf.

Insofern ist für Thüringen die Streitfrage entschieden, ob jede anlassbezogene Datenübermittlung gemäß § 11 Abs. 4 RBStV einer eigenen Regelung in einer Meldeverordnung oder einer Meldedatenübermittlungsverordnung bedarf. Interessant aus Aufsichtsperspektive ist diese Frage allemal, denn sie hat aus Sicht der Kommunen durchaus praktische Auswirkungen.

9 Rundfunkdatenschutzkonferenz (RDSK)

Die Rundfunkdatenschutzbeauftragten haben sich in der Rundfunkdatenschutzkonferenz (RDSK) zusammengeschlossen. Im Berichtsjahr bestand die RDSK aus vier Personen, die die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk über die Rundfunkanstalten und deren Gemeinschaftseinrichtungen und Beteiligungsunternehmen ausüben. Die Mitglieder der RDSK können dem Anhang 13.5 entnommen werden. Im Berichtsjahr haben Sitzungen der RDSK am 07.05.2025 und am 10.11.2025 stattgefunden.

9.1 Aufgaben der RDSK

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

Datenschutzaufsicht über Gemeinschaftseinrichtungen zu einer Verwaltungsvereinbarung zusammengefasst, die Anfang 2024 in Kraft trat. [12].

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

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

- Berichte aus dem AK Medien, dem AK KI, dem AK Grundsatz und dem AK Technik
- Austausch mit den staatlichen Aufsichten im Rahmen der Vorgabe des § 18 BDSG
- Austausch mit Datenschutzaufsichten der privaten Medien
- Erweiterung des RDSK-Papiers zum Data Privacy Framework und digitaler Souveränität
- Auftragsverarbeitung und Informationen über Auftragsverarbeiter
- Austausch zum Audit Redaktionsdatenschutz des RDSB
- Auseinandersetzung mit den sich aus dem Reformstaatsvertrag ergebenen Datenschutzthemen
- Streaming und Aufzeichnung von betrieblichen Versammlungen
- Haltung der RDSK zur US-amerikanischen Datenschutzpolitik

Auf Grundlage des Reformstaatsvertrags wird es ab dem Jahr 2026 allein den gemeinsamen Rundfunkdatenschutzbeauftragten und den Beauftragten für den Datenschutz der Deutschen Welle als Aufsichtsbehörden im öffentlich-rechtlichen Rundfunk in Deutschland geben. Ein Austausch wird regelmäßig stattfinden, sicher nicht in der bisherigen Form.

Die RDSK konnte schnell auf aktuelle Entwicklungen und datenschutzrechtliche Themen reagieren und hatte sich in der bisherigen Form bewährt. Auch als Gegengewicht zu den staatlichen Aufsichtsbehörden hat sie ihren Zweck erfüllt. Ich bedauere, dass es dieses Gremium in Zukunft so nicht mehr geben wird und freue mich umso mehr, dass der Austausch mit dem AK DSB (Arbeitskreis der Datenschutzbeauftragten) auch weiterhin möglich bleibt. Ich bedanke mich an dieser Stelle ausdrücklich bei allen ehemaligen RDSK-Mitgliedern für die kollegiale und immer fachlich fundierte Zusammenarbeit.

9.2 Handreichungen, Empfehlungen und Orientierungshilfen

Gemäß der Geschäftsordnung der Rundfunkdatenschutzkonferenz erstellt und veröffentlicht die RDSK Orientierungshilfen, Handreichungen und Positionspapiere zu datenschutzrelevanten

[12] Siehe Kapitel 13.6 im Anhang

fachlichen, technischen und organisatorischen Fragestellungen. Im Berichtszeitraum wurden folgende Dokumente neu erarbeitet beziehungsweise nachgeschärft.

9.2.1 Stellungnahme zur Informationsplicht des Verantwortlichen über Auftragsverarbeiter und Unterauftragsverarbeiter im Sinne von Art. 28 DSGVO

Im Berichtszeitraum befasste sich die Rundfunkdatenschutzkonferenz (RDSK) mit der Frage, in welchem Umfang Verantwortliche gemäß Art. 28 DSGVO über eingesetzte Auftragsverarbeiter und Unterauftragsverarbeiter informieren müssen. Anlass war unter anderem eine Stellungnahme des Europäischen Datenschutzausschusses (EDSA) aus dem Oktober 2024[13], die zentrale Anforderungen an Transparenz und Rechenschaftspflicht bei der Nutzung von Dienstleistern konkretisiert.

Der EDSA betont, dass Verantwortliche jederzeit, vollständig und leicht verfügbar über die Identität aller beteiligten Auftragsverarbeiter und Unterauftragsverarbeiter verfügen müssen. Dies umfasst insbesondere Name, Adresse sowie eine Kontaktperson. Diese Transparenz ist erforderlich, um den Anforderungen des Art. 28 DSGVO gerecht zu werden.

Aus der EDSA-Stellungnahme leitete die RDSK in einer Stellungnahme vom 19. Dezember 2025 folgende Anforderungen für Verantwortliche ab:

- **Vollständige Identifizierung aller Dienstleister:** Verantwortliche müssen die Identität sämtlicher Auftragsverarbeiter und Unterauftragsverarbeiter kennen, unabhängig vom Risikoniveau der Verarbeitung.
- **Genehmigungspflichten:** Die Einschaltung von Unterauftragsverarbeitern durch den Hauptauftragsverarbeiter erfordert eine spezifische oder allgemeine schriftliche Genehmigung des Verantwortlichen (Art. 28 Abs. 2 DSGVO).
- **Aktualität der Informationen:** Verantwortliche müssen darauf hinwirken, dass Auftragsverarbeiter Änderungen in ihrer Unterbeauftragten-Struktur proaktiv melden.
- **Transparenz gegenüber Betroffenen:** Im Rahmen der Informationspflichten nach Art. 13 f. DSGVO ist über Empfänger bzw. Kategorien von Empfängern zu informieren. Bei Auskunftsverlangen nach Art. 15 DSGVO ist die konkrete Identität der Empfänger mitzuteilen (vgl. EuGH, C-154/21).
- **Berücksichtigung im Verarbeitungsverzeichnis:** Informationen über Empfänger oder Kategorien von Empfängern müssen in das Verarbeitungsverzeichnis nach Art. 30 DSGVO aufgenommen werden.

[13] https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_de

Zur Sicherstellung der DSGVO-Konformität empfiehlt die RDSK:

1. **Prüfung der Auftragsverarbeitungsverträge (AVV):** AVV sollten vollständig dokumentieren, welche Unterauftragsverarbeiter eingesetzt werden. Die entsprechenden Verträge müssen nicht vorgelegt werden, sofern keine Zweifel an der Weitergabe der Datenschutzpflichten bestehen.
2. **Einfordern umfassender Transparenz vom Auftragsverarbeiter**: Auftragsverarbeiter sollten verpflichtet werden, sämtliche Unterauftragsverarbeiter zu benennen und laufend zu aktualisieren.
3. **Zentrale Erfassung aller Dienstleister:** Verantwortliche sollten die Informationen über alle eingesetzten (Unter-)Auftragsverarbeiter so vorhalten, dass unverzügliche Auskünfte gemäß DSGVO jederzeit möglich sind – entweder in einem separaten Register oder integriert in das Verarbeitungsverzeichnis.

9.2.2 Empfehlungen zum Umgang mit dem Data Privacy Framework (DPF) – Version 2.0 mit Hinweisen zur Digitalen Souveränität

In meinem Tätigkeitsbericht 2023 (dort Kapitel 7.2.2) berichtete ich bereits über die von der RDSK veröffentlichte Empfehlung zum Umgang mit dem Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der Europäischen Union und den USA – Trans-Atlantic Data Privacy Framework (DPF).

Der Angemessenheitsbeschluss bestätigt, dass die USA für nach dem DPF zertifizierte Unternehmen ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet. Grundlage bleibt ein Datenschutzniveau, das dem der Europäischen Union vergleichbar sein soll.

Wie bereits in der ersten Version der RDSK-Empfehlungen dargestellt, bestehen allerdings erhebliche Zweifel, ob die im DPF vorgesehenen Garantien den Anforderungen des EuGH dauerhaft standhalten können. Sowohl das Safe Harbor Abkommen als auch das Privacy Shield (beides Vorgänger des DPF) wurden 2015 und 2020 durch den EuGH für unwirksam erklärt. Auch für das DPF ist aufgrund der unverändert bestehenden Bedenken nicht ausgeschlossen, dass ein erneutes gerichtliches Verfahren (dazu Kapitel 3.6.2) erfolgreich sein kann.

Die im August 2025 veröffentlichte Version 2.0 der RDSK-Empfehlung trägt aktuellen politischen und technischen Entwicklungen Rechnung.

Die RDSK weist darin ausdrücklich darauf hin, dass das durch den Angemessenheitsbeschluss erreichte Datenschutzniveau durch die aktuelle US-Regierungspolitik erheblich gefährdet ist. Dies

hat die RDSK veranlasst, ihre bisherigen Empfehlungen zu erweitern und zu konkretisieren. Vor diesem Hintergrund bekräftigt die RDSK, dass Verantwortliche weiterhin Standardvertragsklauseln (SCC) vereinbaren sollten – selbst dann, wenn das DPF und der Angemessenheitsbeschluss formal gelten. Ohne diese Absicherung besteht ein erhöhtes Risiko eines rechtlich ungesicherten Datentransfers, sollte das DPF unwirksam werden.

Neu aufgenommen in die Version 2025 wurde eine Bewertung der digitalen Abhängigkeit der Rundfunkanstalten von US-Clouddiensten. Die RDSK macht deutlich, dass der Einsatz US-amerikanischer Cloud-Infrastruktur angesichts der politischen Unsicherheiten zu erheblichen Risiken für die Vertraulichkeit sensibler Daten führt. Hervorgehoben werden:

- Der CLOUD Act, der US-Behörden Zugriff auf Daten von Unternehmen mit US-Bezug ermöglicht – unabhängig davon, ob die Daten physisch in der EU gespeichert sind.
- Die Gefahr, dass US-Behörden damit auf interne organisatorische Informationen, aber auch auf journalistische Inhalte zugreifen könnten.
- Das Risiko politisch motivierter Eingriffe, wie im Jahr 2025 sichtbar wurde, als Microsoft im Rahmen von Trump-Sanktionen das E-Mail-Konto des Chefanklägers des Internationalen Strafgerichtshofs sperrte.

Auf dieser Basis kam die RDSK zum Schluss, ihre bisherigen Empfehlungen zu erweitern und den Rundfunkanstalten zu empfehlen, die digitale Souveränität zu stärken, insbesondere durch:

- den Aufbau eigener unabhängiger digitaler Infrastrukturen,
- den verstärkten Einsatz von Open-Source-Software,
- die Nutzung und Förderung europäischer Cloud-Lösungen,
- Kompetenzaufbau/Investitionen in Aus- und Weiterbildung,
- hybride Strategien (europäische Cloud + On-Premise),
- Zusammenarbeit mit anderen öffentlichen Einrichtungen,
- Strategien zur Rückholbarkeit von Daten sowie
- klare Notfall- und Krisenmechanismen.

Die RDSK hat mit der Version 2.0 der Empfehlung auf die veränderten Rahmenbedingungen reagiert. Die aktualisierte Fassung trägt der geopolitischen Lage, den anstehenden juristischen Unsicherheiten und der zunehmenden digitalen Abhängigkeit der öffentlich-rechtlichen Rundfunkanstalten Rechnung. Damit stellt die RDSK – wie bereits im Jahr 2023 – ein praxisnahes und aktuelles Instrument zur Verfügung, das die Rundfunkanstalten unterstützt, auch unter unsicheren Bedingungen datenschutzkonform zu handeln und Risiken zu reduzieren.

10 Austausch mit dem Arbeitskreis der Datenschutzbeauftragten (AK DSB)

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

Der AK DSB ist der Arbeitskreis der internen oder betrieblichen Datenschutzbeauftragten des öffentlich-rechtlichen Rundfunks. Zumindest ist er das nach der neugefassten Geschäftsordnung. Die Aufsicht hat nunmehr einen Gaststatus und soll regelmäßig zu den Sitzungen eingeladen werden. Ich halte diese Trennung für vernünftig, da es den betrieblichen Datenschutzbeauftragten möglich sein muss, auch ohne aufsichtsrechtliche Begleitung Themen offen und vertrauensvoll zu diskutieren. Wie sich dies im Jahr 2026 gestalten wird, muss noch besprochen werden.

Im Berichtsjahr hingegen war alles noch beim Alten, und ich habe an den Sitzungen teilgenommen, die in Köln beim WDR und in Bern bei der SRG (Schweizerische Radio- und Fernsehgesellschaft) Rundfunk stattgefunden haben. Thematisiert wurde der Umgang mit Künstlicher Intelligenz und über Projekte in den Rundfunkanstalten dazu berichtet. Microsoft 365 war ein Thema und ebenso weitere Anwendungen in den Anstalten. Auch wurden die Folgerungen aus dem Reformstaatsvertrag besprochen sowie die Auskunftserteilung seitens des Beitragsservice. Einzelthemen wie der Umgang mit Führungszeugnissen und die Überarbeitung des Muster-AVV waren Gegenstände der Beratungen.

In Bern habe ich überdies die Datenschutzmanagement-Checkliste vorgestellt, mit der die Weiterentwicklung und Konsolidierung eines solchen Systems unterstützt und nachgehalten werden kann (siehe auch Kapitel 7.1).

Inwieweit weiterhin aus dem AK DSB durch den Rundfunkdatenschutzbeauftragten berichtet werden sollte, wird ebenso Gegenstand auch der Beratungen im AK DSB mit den internen Datenschutzbeauftragten sein.

11 Austausch mit der Datenschutzkonferenz (DSK)

Die Datenschutzaufsichtsbehörden der Länder und ebenso die Bundesdatenschutzbeauftragte müssen nach dem Bundesdatenschutzgesetz in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der DSGVO zusammenarbeiten. In diesem Zusammenhang sind

auch die nach Art. 85 und Art. 91 der DSGVO eingerichteten Aufsichtsbehörden zu beteiligen. Daher treffen Vertreterinnen und Vertreter der Bundesdatenschutzbeauftragten, der Landesdatenschutzbeauftragten mit den (ab 2026 dem) Rundfunkdatenschutzbeauftragten, den Aufsichten über den privaten Rundfunk sowie den Aufsichten der evangelischen und katholischen Kirche zusammen. Im Berichtsjahr 2025 fand eine Sitzung am 19.03.2025 bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit statt sowie eine weitere Sitzung am 17.12.2025, die als Videokonferenz veranstaltet wurde.

Thematisiert wurden Berichte aus dem Europäischen Datenschutzausschuss und ebenso wurde über die Struktur der Datenschutzaufsicht der Evangelischen Kirche berichtet. Sehr interessant war auch eine Information über den seinerzeitigen Stand der Verhandlungen zum Thema Microsoft 365.

Ich selbst hatte einen Tagesordnungspunkt mit dem Ziel der Verbesserung der Zusammenarbeit der DSK mit den sog. spezifischen Aufsichtsbehörden eingereicht. Es sollten die Gründe für die offensichtliche Zurückhaltung der DSK erörtert und Vereinbarungen getroffen werden mit dem Ziel eines standardisierten und einheitlichen Prozesses der Zusammenarbeit mit der DSK und in den Arbeitskreisen der Datenschutzkonferenz. Gefordert hatte ich:

- Einräumung eines Gaststatus jeder Aufsichtsbehörde im Rahmen der DSK
- Mitarbeit in den Arbeitskreisen, insbesondere AK Medien, AK Grundsatz, AK Technik und AK KI, wobei sämtliche Beratungsunterlagen und der vorbereitete Schriftverkehr vollständig übermittelt werden
- Eine Vereinbarung von Kriterien für Angelegenheiten, in denen eine enge Einbindung wünschenswert ist, mindestens aber eines Verfahrens zur Identifikation solcher Fälle

Hingewiesen habe ich auf das Positionspapier der RDSK zur Zusammenarbeit der nationalen Aufsichtsbehörden, das bereits aus dem Jahr 2021 stammt, und Eckpunkte einer möglichen Zusammenarbeit skizziert hatte. Ich habe bemängelt, dass es nur teilweise gelungen ist, die Zusammenarbeit auf eine tragfähige und für alle Beteiligten befriedigende Basis zu stellen. Hingewiesen habe ich auch auf die kohärente Aufsichtspraxis, der die DSGVO einen hohen Stellenwert zumisst. Das Gebot der Zusammenarbeit ist möglichst weit und nicht möglichst eng auszulegen. Gewünscht hatte ich mir einen Austausch über konkrete Schritte, die unternommen werden, um sowohl dem Gedanken der Zusammenarbeit als auch dem Status der nicht-staatlichen Aufsichtsbehörden Rechnung zu tragen.

Die sehr offene und angenehme Diskussion führte allerdings nicht zu sämtlichen gewünschten Ergebnissen. Ein Gaststatus in der DSK wurde den sogenannten spezifischen Aufsichtsbehörden nicht eingeräumt, konkrete Zusagen zur Verbesserung der Zusammenarbeit in den Arbeitskreisen

jedoch in Aussicht gestellt. Insbesondere soll der Fluss an Informationen und Unterlagen insbesondere zu Beratungsunterlagen der jeweiligen AKs deutlich verbessert werden. Auch der Zugang zu E-Mail-Verteilerlisten wird im Einzelfall verbessert.

Insgesamt kann dieses Ergebnis nicht zufriedenstellen, aber es ist zumindest ein Schritt in die richtige Richtung.

Thematisiert wurden überdies das Data-Privacy-Framework und die notwendigen Anstrengungen zur Erreichung der digitalen Souveränität; ein Thema, das ich eingebracht und Bezug genommen hatte auf die entsprechende Unterlage der RDSK (siehe Kapitel 9.2.2).

11.1 AK Medien

An der Sitzung des AK Medien am 11. und 12. Februar 2025 in Hamburg hat als Vertreterin der RDSK die damalige Rundfunkdatenschutzbeauftragte bei Radio Bremen teilgenommen. An der zweiten Sitzung am 01. und 02. Oktober 2025 konnte mein juristischer Referent online teilnehmen.

Die Sitzungen waren geprägt von der europäischen Regulierung digitaler Dienste sowie der Einordnung neuer Technologien im Spannungsfeld zwischen Datenschutz, Medienfreiheit und Marktregulierung. Aus europäischer Perspektive standen insbesondere die Entwicklungen zu Anonymisierungs- und Pseudonymisierungsmethoden im Mittelpunkt. Die Arbeit des EDSA an Leitlinien zur Abgrenzung anonymer KI-Modelle sowie an Leitlinien zu DMA, Data Act und AI Act wird durch den Arbeitskreis begleitet.

Weiter diskutiert wurde der Einsatz von Tracking-Technologien, namentlich Tracking-Pixeln und sogenannten Tracking-Links sowie die Anerkennung eines Dienstes zur Einwilligungsverwaltung.

Thema war außerdem die geplante Einführung des neuen Fernsehstandards DVB-I, der eine bessere Auffindbarkeit von Programmen ermöglichen soll, datenschutzrechtlich aber Herausforderungen mit sich bringt und deshalb aufmerksam durch die Aufsichtsbehörden begleitet wird. Der Arbeitskreis spricht sich dafür aus, klare datenschutzrechtliche Anforderungen zu formulieren, um den anonymen Zugang zu Rundfunkangeboten sicherzustellen.

Außerdem fand ein Austausch über Zuständigkeit und Befugnisse der Datenschutzaufsichtsbehörden im Bereich der journalistischen Datenverarbeitung anhand § 23 Abs. 2 MStV und damit auch im Rahmen des weit auszulegenden Medienprivilegs statt.

11.2 AK Grundsatz

Auch im Berichtsjahr habe ich am Arbeitskreis Grundsatz der Datenschutzkonferenz teilgenommen. Hier werden insbesondere neue Urteile des EuGH und weitere Themen von grundsätzlicher Bedeutung besprochen.

Es wurden verschiedene Themen im Hinblick auf die Frage der Auslegung und Behandlung des Auskunftsanspruchs aus Art. 15 DSGVO sowie Grundsatzfragen zum Thema berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO und deren Auswirkungen besprochen. Weitere Themen waren die Abberufung eines betrieblichen Datenschutzbeauftragten aus wichtigem Grund sowie eine Diskussion der Frage, ob Auskunftsanträge durch Eltern aus Gründen des Kindeswohls abgelehnt werden können.

Die Sitzungen im Berichtsjahr fanden statt am 18./19. Februar und am 18./19. November 2025, wobei in der letzten Sitzung hauptsächlich Vorschläge aus einer Strategieklausur des AK DSK 2.0 zur Änderung der DSGVO besprochen wurden. Hier war leider übersehen worden, die Aufsichtsbehörden aus Medien und Kirchen über den Inhalt dieser Diskussion in Kenntnis zu setzen, sodass eine Mitarbeit auch während der Sitzung nicht möglich war.

Ungeachtet dieser Kritik ist der Austausch in diesem Gremium sehr angenehm und sollte aufrechterhalten und – auch dies ist ein schon länger gehegter Wunsch – intensiviert werden.

11.3 AK Technik

An den beiden Online-Sitzungen des AK Technik am 25./26. Februar 2025 sowie am 30. September und 1. Oktober 2025 hat meine Referentin für technisch-organisatorische Themen teilgenommen. Neben Berichten zur Zusammenarbeit auf europäischer Ebene (Leitlinienerarbeitung) sowie aus Arbeitsgruppen und Unterarbeitsgruppen des AK Technik fand dort auch ein Austausch zu verschiedenen Themen statt. Spannend war unter anderem der präventive und konstruktive Ansatz des HBDI, datenschutzrechtliche Werkzeuge zur Unterstützung von Behörden und Verantwortlichen als Open Source-Lösung bereitzustellen[14].

Auch die Teilnahme am Informationsaustausch der IT-Labore der Aufsichtsbehörden haben wir weitergeführt. Hier war es uns möglich, am Austausch vom 24.-26. November 2025 in Magdeburg teilzunehmen, während der Termin vom 12.-14. Mai 2025 in Wiesbaden für uns kapazitätsbedingt

[14] siehe dazu auch HBDI veröffentlicht Programmcode auf OpenCode.de | datenschutz.hessen.de

entfallen musste. Die Zusammenkunft in Magdeburg bot erneut einen intensiven fachlichen Austausch, kollegiale Unterstützung sowie einen wertvollen Wissenstransfer. Auch Behörden, die noch nicht über ein eigenes IT-Labor verfügen oder sich im Aufbau eines solchen befinden, waren eingeladen, eigene Fragestellungen einzubringen und an den Erfahrungen bestehender IT-Labore teilzuhaben. Für unsere Behörde bleibt in naher Zukunft insbesondere die Durchführung von App-Prüfungen in einer IT-Labor-Umgebung ein zentraler Schwerpunkt. Hierfür ist der weitere Aufbau der erforderlichen personellen und technischen Ressourcen notwendig.

11.4 AK KI

Wie im letzten Tätigkeitsbericht bereits informatorisch erwähnt, wurde im Jahr 2025 der AK Künstliche Intelligenz als neuer Arbeitskreis der DSK ins Leben gerufen. Ich konnte an der konstituierenden Sitzung am 23./24. Januar 2025 in Mainz teilnehmen. Mein Referent nahm an der zweiten Sitzung am 23./24. September in Stuttgart teil.

Der Arbeitskreis dient der Bündelung fachlicher Expertise im Bereich Künstlicher Intelligenz und soll als Schnittstelle zur europäischen Ebene fungieren. Besonderer Fokus soll dabei auf Betroffenenrechte und Transparenz beim Einsatz von KI-Systemen sowie auf die Rechtsgrundlagen und Zulässigkeit des Einsatzes von rechtswidrig trainierten KI-Modellen gerichtet werden. Darüber hinaus beabsichtigt der Arbeitskreis, die technische und rechtliche Entwicklung im Bereich der KI-Forschung kontinuierlich zu beobachten und einschlägige regulatorische Initiativen auf europäischer wie auch auf internationaler Ebene in den Blick zu nehmen.

In der zweiten Sitzung wurden insbesondere Fragen der Anwendbarkeit der DSGVO und der Transparenzanforderungen bei Trainingsdaten diskutiert. Zudem wurde über den Stand der Arbeiten an gemeinsamen EU-Leitlinien zum Zusammenspiel von KI-Verordnung und DSGVO berichtet. Thema waren darüber hinaus die Erarbeitung eines Papiers zu „Retrieval Augmented Generation AI“ (RAG) und die Vorbereitung einer Stellungnahme zur Marktüberwachung nach der KI-Verordnung. Auch Fragen zum Einsatz von KI im öffentlichen Bereich waren Gegenstand der Sitzung.

Wie in den anderen Arbeitskreisen der DSK werden die unabhängigen Aufsichtsbehörden der Medien und Kirchen bedauerlicherweise auch hier nicht als vollwertiges Mitglied anerkannt. Es ist zwar zu begrüßen, dass meine Behörde neben den regulären Sitzungen auch am monatlichen Jour fixe des AK KI teilnehmen kann, um einen Einblick in die Arbeit des Arbeitskreises zu erhalten. Eine aktivere Mitarbeit (im Rahmen unserer Kapazitäten) ist jedoch nicht erwünscht und ohne Kenntnis der Inhalte, die über den internen E-Mail-Verteiler des Arbeitskreises kommuniziert werden, auch

kaum möglich. Die Teilnahme am AK KI ist aber nicht zuletzt vor dem Hintergrund der rasanten Entwicklung in diesem Bereich unabdingbar.

12 Ausblick und Schlussbemerkung

Die institutionalisierte gemeinsame Rundfunkdatenschutzaufsicht hat mit Beginn des Jahres 2026 ihre Tätigkeit aufgenommen. Die ersten Monate haben bereits gezeigt, dass ein erheblich höherer Aufwand betrieben werden muss, insbesondere im Hinblick auf die Bearbeitung von Beschwerden. Künstliche Intelligenz ist aus dem gesellschaftlichen Alltag nicht mehr wegzudenken und prägt zunehmend auch die Art und Weise, wie Eingaben an Aufsichtsbehörden erfolgen. Vor diesem Hintergrund ist es erforderlich, dass sich auch die Aufsicht selbst aktiv mit den veränderten Rahmenbedingungen auseinandersetzt. Es ist zu prüfen, wie mit künftig verstärkt KI-gestützt erstellten Eingaben umzugehen ist, welche Auswirkungen dies auf Prüfungsmaßstäbe, Verfahrensabläufe und Ressourcen hat und inwieweit ein eigener, verantwortungsvoller Einsatz von KI-Werkzeugen zur Unterstützung der Aufgabenerfüllung in Betracht kommt. Maßgeblich bleiben dabei Transparenz, Nachvollziehbarkeit, rechtliche Verlässlichkeit sowie die Wahrung der Rechte betroffener Personen. Der Einsatz von KI kann die Aufsichtstätigkeit unterstützen, ersetzt jedoch weder die rechtliche Bewertung im Einzelfall noch die eigenständige pflichtgemäße Entscheidung der Aufsichtsbehörde.

Vorgenommen für das Jahr 2026 habe ich mir, zunächst alle Beteiligungsunternehmen der Rundfunkanstalten in den Blick zu nehmen und eine Querschnittsprüfung durchzuführen, die einen Überblick über den Stand der Datenschutzumsetzung dort geben soll. Weiterhin sehe ich mich veranlasst, den Personaldatenschutz in den von mir beaufsichtigten Rundfunkanstalten zu prüfen. Auch wenn es noch keine gesetzliche Grundlage zum Beschäftigtendatenschutz gibt (siehe Kapitel 3.4 des Tätigkeitsberichts 2024), möchte mir dennoch einen Eindruck davon verschaffen, wie Datenschutz in den Personalabteilungen und -bereichen umgesetzt und gelebt wird.

Weiterverfolgen werde ich auch die (Weiter-)Entwicklung der Datenschutzmanagementsysteme in den Rundfunkanstalten. Die in Kapitel 7.1 dargestellten Checklisten zur Handreichung Datenschutzmanagement-Check sollen als ein lebendiges Steuerungsinstrument und zur Nachweisführung hin zu einem wirksamen Datenschutzmanagementsystem dienen.

Die Herausforderungen, die der Reformstaatsvertrag an die Digitalisierung der Anstalten und die gemeinsamen Anstrengungen adressiert, sind in Teilen datenschutzrechtlicher Natur. Hier wird es darauf ankommen, die richtigen Weichenstellungen zu setzen. Die Aufsicht sieht sich in der Verantwortung und der Pflicht, daran mitzuwirken. Themen sind Umgang mit personenbezogenen

Daten zum Zweck der Auftragserfüllung, Austausch personenbezogener Daten auf Basis des gemeinsamen technischen Plattformsystems, datensichere und datensparsame Personalisierungsmöglichkeiten und Empfehlungssysteme mit einer öffentlich-rechtlichen Zielsetzung und Ausgestaltung. Ein weiterer wichtiger Anknüpfungspunkt für datenschutzrechtliche Überlegungen ist gewiss die Verpflichtung der Anstalten, Kennzahlen und Verfahren zu entwickeln, die Leistungsanalysen ermöglichen. Hier wird es darauf ankommen, dass diese Verpflichtung nicht als Freifahrtschein der Anstalten betrachtet wird, Daten jenseits der datenschutzrechtlichen Grenzen zu nutzen. Aufgrund der Unabhängigkeit der Aufsicht bin ich dafür verantwortlich, die gesetzeskonforme Umsetzung des Aufgabenkatalogs auch aus der DSGVO sicherzustellen.

Um sich weiterhin einzumischen und aktiv an der Gestaltung des Datenschutzes im öffentlich-rechtlichen Rundfunk mitzuwirken, bedarf es einer spürbaren Stärkung der Aufsicht in personeller Hinsicht. Auch wenn dies in Zeiten angespannter Haushalte eine Forderung sein dürfte, die auf ein geteiltes Echo stößt, muss doch in aller Deutlichkeit darauf hingewiesen werden, dass die Aufsicht nur dann ihren gesetzlich vorgeschriebenen Aufgaben nachkommen kann, wenn Sie dementsprechend ausgestattet ist.

Ich bedanke mich bei allen Landesrundfunkanstalten, dem ZDF und Deutschlandradio, den Rundfunk-, Fernseh- und Hörfunkräten sowie den Verwaltungsräten und natürlich ebenso bei den Geschäftsleitungen für die stets respektvolle und wertschätzende Zusammenarbeit. Ich bin sicher, dass dies auch im Jahr 2026 so fortgeführt wird. Zugleich hoffe ich, dass die inzwischen zentral ausgestaltete Datenschutzaufsicht als unterstützende und maßgebliche Instanz des Datenschutzes im öffentlich-rechtlichen Rundfunk wahrgenommen wird.

Vor diesem Hintergrund blicke ich dem vor uns liegenden Jahr und den anstehenden Herausforderungen zuversichtlich entgegen.

13 Anhang

13.1 DSGVO Art. 51 ff.

Artikel 51

Aufsichtsbehörde

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

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

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

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

Artikel 52

Unabhängigkeit

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

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

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

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

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

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

Artikel 55

Zuständigkeit

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

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

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

Artikel 57

Aufgaben

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

a) die Anwendung dieser Verordnung überwachen und durchsetzen;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

s) verbindliche interne Vorschriften gemäß Artikel 47 genehmigen;

t) Beiträge zur Tätigkeit des Ausschusses leisten;

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

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

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

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

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

Artikel 58

Befugnisse

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

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

b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

e) Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren,

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

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

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

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

j) verbindliche interne Vorschriften gemäß Artikel 47 zu genehmigen.

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

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

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

Artikel 59

Tätigkeitsbericht

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

13.2 DSGVO Art. 85

Artikel 85

Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

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

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

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

13.3 MStV – §§ 12, 23, 31j ff., 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.

---

§ 31j

Gemeinsamer Rundfunkbeauftragter für den Datenschutz

(1) Die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF und das Deutschlandradio ernennen einen gemeinsamen Rundfunkbeauftragten für den Datenschutz (Rundfunkdatenschutzbeauftragter), der zuständige Aufsichtsbehörde im Sinne des Artikels 51 der Verordnung (EU) 2016/679 ist. Die Ernennung erfolgt durch die Rundfunkräte der in der ARD zusammengeschlossenen Landesrundfunkanstalten, den Fernsehrat des ZDF und den Hörfunkrat des Deutschlandradios für die Dauer von acht Jahren; Wiederernennungen sind zulässig. Der Rundfunkdatenschutzbeauftragte muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, nachgewiesen durch ein abgeschlossenes Hochschulstudium, sowie über Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Das Amt des Rundfunkdatenschutzbeauftragten kann nicht neben anderen Aufgaben innerhalb der in der ARD zusammengeschlossenen Landesrundfunkanstalten, des ZDF und des Deutschlandradios und der jeweiligen Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt des Rundfunkdatenschutzbeauftragten zu vereinbaren sein und dürfen 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. Der Rundfunkdatenschutzbeauftragte kann seines Amtes nur enthoben werden, wenn er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt. Dies erfolgt durch Beschluss der Rundfunkräte der in der ARD zusammengeschlossenen Landesrundfunkanstalten, des Fernsehrats des ZDF und Hörfunkrats des Deutschlandradios. Der Rundfunkdatenschutzbeauftragte ist vor der Entscheidung zu hören.

(3) Das Nähere, insbesondere die Grundsätze der Vergütung, regeln die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF und das Deutschlandradio in einer gemeinsamen Satzung (gemeinsame Satzung über die Datenschutzaufsicht der Rundfunkanstalten). Die in der ARD zusammengeschlossenen Landesrundfunkanstalten legen entsprechend der Bestimmungen des II. und III. Abschnitts des ARD-Staatsvertrages eine federführende Anstalt fest.

---

§ 31k

Unabhängigkeit

(1) Der Rundfunkdatenschutzbeauftragte ist in Ausübung des Amtes unabhängig und nur dem Gesetz unterworfen. Er unterliegt keiner Rechts- oder Fachaufsicht. Der Dienstaufsicht unterliegt er, soweit die Unabhängigkeit bei der Ausübung des Amtes dadurch nicht beeinträchtigt wird. Die Dienstaufsicht wird durch den Verwaltungsrat der Rundfunkanstalt am Dienstsitz wahrgenommen.

(2) Dem Rundfunkdatenschutzbeauftragten ist eine Dienststelle einzurichten (Dienstsitz). Für die Erfüllung der Aufgaben und Befugnisse sind ihm die notwendigen Personal-, Finanz- und Sachausstattung zur Verfügung zu stellen. Die erforderlichen Mittel sind jährlich, öffentlich und gesondert im Haushaltsplan der Rundfunkanstalt am Dienstsitz auszuweisen und dem Rundfunkdatenschutzbeauftragten im Haushaltsvollzug zuzuweisen. Einer Finanzkontrolle des entsprechend Absatz 1 Satz 4 zuständigen Verwaltungsrates unterliegt der Rundfunkdatenschutzbeauftragte nur, soweit die Unabhängigkeit bei der Ausübung des Amtes dadurch nicht beeinträchtigt wird.

(3) Einzelheiten zur Ausführung der Absätze 1 und 2 regeln die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF und das Deutschlandradio in der gemeinsamen Satzung über die Datenschutzaufsicht der Rundfunkanstalten.

(4) Der Rundfunkdatenschutzbeauftragte ist in der Wahl der Mitarbeiter frei. Sie unterstehen allein seiner Leitung.

---

§ 31l

Aufgaben und Befugnisse

(1) Der Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Datenschutzvorschriften dieses Staatsvertrages, der Verordnung (EU) 2016/679, der §§ 19 bis 25 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit der in der ARD zusammengeschlossenen Landesrundfunkanstalten, des ZDF und des Deutschlandradios sowie ihrer Beteiligungsunternehmen im Sinne des § 42 Abs. 3 Satz 1. Er hat die Aufgaben und Befugnisse entsprechend den Artikeln 57 und 58 Abs. 1 bis 5 der Verordnung (EU) 2016/679. Bei der Zusammenarbeit mit anderen Aufsichtsbehörden hat er, soweit die Datenverarbeitung zu journalistischen Zwecken betroffen ist, den lnformantenschutz zu wahren. Er kann gegenüber den in der ARD zusammengeschlossenen Landesrundfunkanstalten, dem ZDF und dem Deutschlandradio keine Geldbußen verhängen.

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

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

(4) Der Rundfunkdatenschutzbeauftragte erstattet jährlich auch den Organen der in der ARD zusammengeschlossenen Landesrundfunkanstalten, des ZDF und des Deutschlandradios schriftlichen Bericht im Sinne des Artikels 59 der Verordnung (EU) 2016/679 über seine Tätigkeit. Der Bericht wird veröffentlicht, wobei eine Veröffentlichung im Online-Angebot der in der in der ARD zusammengeschlossenen Landesrundfunkanstalten, des ZDF und des Deutschlandradios ausreichend ist.

(5) Jedermann hat das Recht, sich unmittelbar an den Rundfunkdatenschutzbeauftragten zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine der in der ARD zusammengeschlossene Landesrundfunkanstalten, das ZDF, das Deutschlandradio oder ihre Beteiligungsunternehmen im Sinne des § 42 Abs. 3 Satz 1 in seinen schutzwürdigen Belangen verletzt zu sein.

(6) Der Rundfunkdatenschutzbeauftragte ist sowohl während als auch nach Beendigung seiner Tätigkeit verpflichtet, über die ihm während seiner Dienstzeit bekannt gewordenen Angelegenheiten und vertraulichen Informationen Verschwiegenheit zu bewahren.

---

§ 113

Datenschutzaufsicht bei Telemedien

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

13.4 TDDDG § 25

§ 25 TDDDG

Schutz der Privatsphäre bei Endeinrichtungen

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

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

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

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

13.5 RDSK-Mitgliederliste 2025

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 Florian Wagenknecht	DW - Deutsche Welle
Dr. Heiko Neuhoff	NDR - Norddeutscher Rundfunk
Ivka Jurčević	RB - Radio Bremen

13.6 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.

§ 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

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

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

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