Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten für das Jahr 2019

Der Rundfunkdatenschutzbeauftragte
Von BR, SR, WDR, Deutschlandradio, ZDF
Marlene-Dietrich-Allee 20
14482 Potsdam

Tel 0331 97980 85500
Fax 0331 97980 85509
kontakt@rundfunkdatenschutz.de
www.rundfunkdatenschutz.de

Vorwort

Dies ist der erste Bericht über die Tätigkeit eines gemeinsamen Rundfunkdatenschutzbeauftragten für mehrere Rundfunkanstalten. Die für diese Einrichtung maßgeblichen gesetzlichen Grundlagen und die entsprechenden Aufsichtsfunktionen bestehen zwar bereits seit dem 25. Mai 2018. In ihrer spezifischen Konfiguration und Konstruktion gibt es die Datenschutzaufsicht durch einen gemeinsamen Rundfunkdatenschutzbeauftragten jedoch erst seit Beginn des Jahres 2019. Der Tätigkeitsbericht umfasst daher nur dieses Jahr und ist zugleich ein Erfahrungsbericht in mehrfacher Hinsicht:

- Mit Inkrafttreten der DSGVO ist in Bezug auf die genannten fünf Rundfunkanstalten das Neben- und Miteinander von Datenschutzaufsicht und internen Datenschutzbeauftragten neu geregelt worden, insbesondere mit Blick auf die völlige Unabhängigkeit der Aufsichtsfunktion.
- Die originäre Zuständigkeit für die Einrichtung der Datenschutzaufsicht übertragen die neuen Rechtsgrundlagen erstmals vollständig den Gremien der Rundfunkanstalten.
- Erstmals haben sich die zuständigen Gremien mehrerer Rundfunkanstalten auf die Einrichtung bzw. Wahl einer gemeinsamen Datenschutzaufsicht verständigt.
- Der Amtssitz des auf dieser Grundlage mandatierten gemeinsamen Rundfunkdatenschutzbeauftragten befindet sich erstmals nicht nur rechtlich, sondern auch personell und räumlich außerhalb des Organisationsgefüges der zu beaufsichtigenden Einrichtungen.
- Schließlich und ganz allgemein hat das Inkrafttreten der DSGVO dem Datenschutz zu enormer Popularität verholfen, die Sensibilität in der Bevölkerung erhöht und eine Vielzahl neuer Fragen zum Verständnis und zur Umsetzung des Datenschutzrechts aufgeworfen, die sich in einer entsprechend gestiegenen „Nachfrage“ bei der Datenschutzaufsicht niedergeschlagen haben.

All dies hat die Aktivitäten des zurückliegenden Jahres geprägt und wird deshalb Gegenstand dieses Berichts sein. Er soll zugleich dazu dienen, meine Rechtsauffassung zu wichtigen Themen des Datenschutzes bzw. der Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk zu erläutern und auf diese Weise auch den Verantwortlichen Orientierungspunkte für meine Aufsichtspraxis geben.

Den für meine Wahl bzw. Bestellung verantwortlichen Gremien der fünf Rundfunkanstalten danke ich dafür, dass sie mir ver- und zugetraut haben, diese neue Funktion im Sinne der gesetzlichen Vorgaben und ihrer eigenen Erwartungen an eine effektive und effiziente Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk wahrzunehmen. Den Mitgliedern der Gremiengeschäftsstellen danke ich für ihre verlässliche Unterstützung und zugewandte Hilfsbereitschaft. Den Datenschutzbeauftragten in meinem Zuständigkeitsbereich danke ich für die stets konstruktive, offene Zusammenarbeit. Und schließlich, aber nicht zuletzt gilt mein besonders herzlicher Dank meinen beiden Kolleginnen, die mit mir in diesem ersten Jahr das kleine Team der gemeinsamen Datenschutzaufsicht für BR, SWR, WDR, Deutschlandradio und ZDF sowie ihre Gemeinschaftseinrichtungen und Beteiligungsgesellschaften gebildet und das damit verbundene Neuland mit mir gemeinsam Schritt für Schritt erschlossen haben.

Potsdam, Februar 2020
Dr. Reinhart Binder

Inhaltsverzeichnis

Hinweis:

Im Text lege ich stets die gesetzlich vorgegebenen Bezeichnungen zugrunde und verzichte im Interesse einer besseren Lesbarkeit weitgehend auf geschlechtsspezifische Formulierungen. Sämtliche Personenbezeichnungen richten sich in gleicher Weise an die Angehörigen aller Geschlechter.

Anders als die drei Landesrundfunkanstalten und das ZDF ist das Deutschlandradio eine Körperschaft öffentlichen Rechts. Im Interesse der besseren Lesbarkeit verwende ich stets einheitlich den Begriff „Rundfunkanstalten".

Einleitung

1 Nach Art. 59 DSGVO erstellt jede Aufsichtsbehörde einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen nach Art. 58 Abs. 2 DSGVO 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 Europäischen Datenschutzausschuss (Art. 68 DSGVO) zugänglich gemacht.

2 Die für mich maßgeblichen Landesrundfunkgesetze bzw. Staatsverträge sehe auf dieser Basis im wesentlichen gleichlautend vor, dass der Rundfunkdatenschutzbeauftragte den Bericht im Sinne von Art. 59 DSGVO jährlich „auch den Organen" der Rundfunkanstalt bzw. Körperschaft erstattet[1]. Ebenfalls gleichlautend sehen alle Vorschriften (entsprechend der Vorgabe von Art. 59 DSGVO) eine Veröffentlichung des Berichts vor, wobei sie eine solche im Onlineangebot der jeweiligen Rundfunkanstalt bzw. Körperschaft für ausreichend erklären. Eine – letztlich deklaratorische - Vorgabe

[1] Art. 21 Abs. 9 BR-Gesetz, § 42d Abs. 5 SMG, § 51 Abs. 5 WDR-Gesetz, §§ 18 Abs. 4 DRadio- bzw. ZDF-Staatsvertrag

zur Veröffentlichung in inhaltlicher Hinsicht enthält lediglich Art. 21 Abs. 9 S. 2 BR-Gesetz; danach hat der Bericht die Betriebs- und Geschäftsgeheimnisse des Bayerischen Rundfunks sowie die personenbezogenen Daten seiner Beschäftigten zu wahren.

3 Nach meinem Verständnis dieser Vorschriften und mit Blick auf das auch für die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk maßgebliche Gebot der Staatsferne erstatte ich diesen Tätigkeitsbericht in erster Linie den Organen der fünf Rundfunkanstalten in meinem Zuständigkeitsbereich. Die jeweiligen Landesregierungen und –parlamente habe ich darauf hingewiesen, dass der Tätigkeitsbericht erschienen ist und auf meiner Homepage zum Download zur Verfügung steht. Damit dürfte dem Sinn und Zweck der einschlägigen Vorgaben hinreichend Rechnung getragen sein. Die Rundfunkanstalten in meinem Zuständigkeitsbereich können den Tätigkeitsbericht ihrerseits, wie nach dem für sie jeweils maßgeblichen Landesrecht ausdrücklich vorgesehen, unmittelbar in ihrem Onlineangebot zur Verfügung stellen. Mindestens aber sollten sie ihren Nutzern den Bericht durch Verlinkung mit meiner Homepage zugänglich machen.

1 Datenschutz und Datenschutzaufsicht: Grundlagen

a Gesetzgebung

aa) Vorab: Datenschutz und Medien

4 Grundsätzlich unterliegen auch Medienanbieter (also Presseverlage sowie öffentlich-rechtliche und private Rundfunk- und Telemedienanbieter) in vollem Umfang dem allgemeinen Datenschutzrecht. Also beispielsweise im Verhältnis zu ihren fest oder frei Beschäftigten, Abonnenten, Nutzern, Kunden, Partnern, Lieferanten etc. pp. Insoweit gibt es keine Besonderheiten gegenüber allen anderen Unternehmen oder Organisationen.

5 Dies gilt jedoch nicht für den Kernbereich ihrer Tätigkeit, nämlich die Datenverarbeitung zu journalistischen Zwecken. Insoweit schreibt Art. 85 Abs. 2 DSGVO vor, dass die Mitgliedstaaten „Abweichungen oder Ausnahmen“ von zahlreichen Kapiteln der DSGVO vorsehen, „wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.“

6 Auf dieser Grundlage beschränkt § 9c Abs. 1 S. 4 und 5 RStV für den öffentlich-rechtlichen und privaten Rundfunk die Vorgaben der DSGVO für die Datenverarbeitung zu journalistischen Zwecken auf einige wenige Abschnitte bzw. Vorschriften der DSGVO. Danach haften die Verantwortlichen nur für eine Verletzung des Da-

tengeheimnisses sowie für unzureichende Maßnahmen zum Schutz der Integrität und Vertraulichkeit der entsprechenden Daten[2]. Entsprechend gilt das gemäß § 9c Abs. 1 S. 6 RStV auch für die jeweiligen Hilfs- und Beteiligungsunternehmen der Rundfunkanstalten bzw. -veranstalter. Der Ausnahmebereich umfasst den gesamten journalistischen Prozess von der Recherche über die Produktion und Speicherung bis hin zur Veröffentlichung. Er wirkt sich damit auf alle Rechtsbeziehungen zwischen Journalisten und Personen sowohl im Vorfeld (soweit die Person Objekt der Recherche oder an ihr – etwa als Informant oder als Interviewpartner – beteiligt ist) als auch nach der Veröffentlichung (als betroffener Hörer, Zuschauer oder Nutzer) aus.

7 Diese weitreichende Freistellung der Datenverarbeitung zu journalistischen Zwecken von den Restriktionen des Datenschutzrechts ist nach deutschem Verfassungsrecht zwingend geboten. Das Bundesverfassungsgericht bezeichnet Rundfunk und Presse als „Medium und Faktor der öffentlichen Meinungsbildung" und zählt sie deshalb zu den elementaren Bestandteilen einer funktionsfähigen demokratischen Gesellschaft. Journalistische Arbeit beruht ganz entscheidend auf dem Sammeln, Bewerten, Verknüpfen und Veröffentlichen von Informationen – meist in Gestalt personenbezogener Daten. Dies gehört zum Wesenskern des Journalismus, gleich ob es um die investigative Recherche und oder allgemeine Berichterstattung geht, und unabhängig vom Genre wie bspw. Kultur, Bildung, Sport oder Unterhaltung.

8 Diese gesamte Datenverarbeitung wäre nach den Vorgaben der DSGVO sowie der nationalen Datenschutzgesetze an und für sich nur unter engen Voraussetzungen zulässig. Denn im allgemeinen ist dafür ein gesetzlicher Erlaubnistatbestand oder eine ausdrückliche Einwilligung des Betroffenen erforderlich. Eine ungefilterte, unbeeinflusste, auch kritische und/oder investigative Recherche und Berichterstattung wäre unter diesen Vorzeichen freilich kaum möglich. Diesem offenkundigen Wertungswiderspruch zwischen Presse- bzw. Rundfunkfreiheit (Art. 5 Abs. 1 S. 2 GG) bzw. Informations- und Meinungsfreiheit (Art. 5 Abs. 1 S. 1 GG) einerseits und dem „Grundrecht auf informationelle Selbstbestimmung" (Art. 2 Abs. 1 GG) andererseits tragen deutsche Gesetzgebung und Rechtsprechung seit langem dadurch Rechnung, dass die Medien von zahlreichen datenschutzrechtlichen Beschränkungen ausgenommen werden, wie dies nun auch Art. 85 DSGVO ausdrücklich vorschreibt. In Deutschland wird dies traditionell als „**Medienprivileg**" bezeichnet. Um

[2] § 9c Abs. 1 S. 4 und 5 RStV:
Im Übrigen finden für die Datenverarbeitung zu journalistischen Zwecken von der [DSGVO] 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 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird.

ein „Privileg“ handelt es sich dabei allerdings nur aus der rein datenschutzrechtlichen Perspektive; für die Funktionsweise der Massenmedien und damit für die demokratische Gesellschaft insgesamt ist ein medienspezifisch angepasster Datenschutz zwingend und konstitutiv, daher gerade kein „Privileg“.

9 Dies bedeutet nicht, dass Journalisten und Redaktionen mit personenbezogenen Daten nach Gutdünken verfahren dürfen. So untersagt es § 9c Abs. 1 S. 1 RStV[3] den Landesrundfunkanstalten, dem ZDF, dem Deutschlandradio und privaten Rundfunkveranstaltern bzw. den mit der journalistischen Datenverarbeitung befassten Personen ausdrücklich, die entsprechenden Daten zu anderen Zwecken zu verarbeiten. Mit dieser als „**Datengeheimnis**“ bezeichneten Verpflichtung geht das deutsche Recht über die Vorgaben der DSGVO hinaus.

10 Dabei fällt für die Rundfunkanstalten besonders ins Gewicht, dass der Bundesgerichtshof[4] ihre Redakteure als Amtsträger qualifiziert hat, die sich im Falle einer Verwendung bestimmter sensibler personenbezogener Daten für nicht-journalistische Zwecke demzufolge sogar nach § 203 Abs. 2 S. 1 Nr. 1 StGB strafbar machen können[5]. Dies unterstreicht, dass dem verfassungsrechtlichen Funktionsauftrag des öffentlich-rechtlichen Rundfunks mit den entsprechenden Privilegien in datenschutzrechtlicher Hinsicht spezifische Gewährleistungsverpflichtungen gegenüberstehen, so wie dies beispielsweise auch für Beamte und andere Berufsgruppen gilt. Die Gesellschaft soll sich auf die besondere Sorgfalt und Umsicht des öffentlich-rechtlichen Rundfunks, den sie finanziert, gerade in Bezug auf seine Berichterstattung und dafür verarbeitete personenbezogene Daten verlassen können – vor allem, aber keineswegs nur, soweit es um besonders sensible personenbezogene Daten geht.

11 Zudem verpflichtet § 9c Abs. 1 S. 4 RStV in Verbindung mit Art. 32 DSGVO die Verantwortlichen im öffentlich-rechtlichen und privaten Rundfunk dazu, für angemessene Vorkehrungen zur **Datensicherheit** zu sorgen. Welche technischen und organisatorischen Maßnahmen dies bedingt, hängt wie stets von vielen Faktoren ab.

12 Konsequenzen hat die spezifische Situation des Rundfunks – insbesondere der Rundfunkanstalten - im Gefüge des deutschen Verfassungsrechts auch für die **Da-**

---

3 *„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).“*

4 BGH, Urteil vom 27.11.2009 – 2 StR 104/09 -

5 Nach dieser Vorschrift wird bestraft, *„wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbart, das ihm als Amtsträger anvertraut oder sonst bekannt geworden ist.“*

tenschutzaufsicht. Auf die damit verbundenen organisatorischen Aspekte gehe ich in Abschnitt 2 näher ein. In inhaltlicher Hinsicht beschränkt § 9c Abs. 1 S. 8 RStV im Bereich der journalistischen Datenverarbeitung die Rechte der Betroffenen auf einige wenige Ansprüche. Namentlich geht es dabei um die Verpflichtung der Rundfunkanstalten, etwaige Gegendarstellung, Verpflichtungserklärungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Dauer aufzubewahren wie die Daten selbst, sowie sie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln (§ 9c Abs. 2 RStV). Außerdem gewährt § 9c Abs. 3 RStV einer durch eine Berichterstattung in ihrem Persönlichkeitsrecht beeinträchtigten Person einen Anspruch auf Auskunft, auf unverzügliche Berichtigung unrichtiger personenbezogener Daten oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang. Die Rundfunkanstalt kann die Auskunft aus den im einzelnen in § 9c Abs. 3 RStV genannten Gründen, die etwa den Informantenschutz gewährleisten sollen, verweigern[6].

13 Diese Ansprüche richten sich naturgemäß an den Verantwortlichen und nicht etwa an die Datenschutzaufsicht. Der Verantwortliche hat also eigenständig zu prüfen, ob die für eine Auskunft oder deren Verweigerung maßgeblichen Voraussetzungen vorliegen. Die betroffene Person kann im Streitfall unmittelbar die Hilfe der Zivilgerichtsbarkeit in Anspruch nehmen, insbesondere auch, um weitere Ansprüche etwa nach § 22 KUG oder § 823 BGB durchzusetzen.

14 Sie kann sich außerdem jedoch gemäß Art. 77 DSGVO alternativ oder kumulativ mit einer Beschwerde an die Datenschutzaufsicht wenden. Diese hat in diesem Fall zumindest die Tragfähigkeit der vom Verantwortlichen genannten Gründe für die Ablehnung des geltend gemachten Anspruchs zu überprüfen. Einen etwaigen Bescheid der Datenschutzaufsicht kann der Beschwerdeführer wiederum verwaltungsgerichtlich überprüfen lassen, Art. 78 Abs. 1 DSGVO. Bislang ungeklärt ist, in welchem Verhältnis zueinander die in einem parallelen Zivil- und Verwaltungsge-

---

6 *Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, kann die betroffene Person Auskunft über die der Berichterstattung zugrunde liegenden, 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.

richtsverfahren ergehenden Entscheidungen stünden, soweit sie beispielsweise zu einer unterschiedlichen Bewertung der Frage gelangen, ob die Berichterstattung das Persönlichkeitsrecht „beeinträchtigt" oder der Verantwortliche zu recht die Auskunft über die Rechercheunterlagen verweigert hat.

15 Hingewiesen sei in diesem Zusammenhang schließlich noch auf die Vorschrift des § 9c Abs. 1 S. 7 RStV. Ihr zufolge können sich die öffentlich-rechtlichen und privaten Rundfunkveranstalter sowie ihre Verbände und Vereinigungen „Verhaltenskodizes geben, die in einem transparenten Verfahren erlassen und veröffentlicht werden." Mit Blick auf ihre systematische Stellung hat die Vorschrift erkennbar primär einen datenschutzrechtlichen Hintergrund. Aus der amtlichen Begründung zum 21. RÄndStV, auf dessen Grundlage die Vorschrift am 25. Mai 2018 in Kraft getreten ist, geht nicht näher hervor, welchen Inhalt oder Charakter ein solcher **Verhaltenskodex** haben, ob er sich etwa beispielsweise am Pressekodex orientieren soll. Sie stellt lediglich klar, dass es dabei nicht etwa um „Verhaltensregeln" im Sinne von Art. 40 DSGVO gehen soll, die von der datenschutzrechtlichen Aufsichtsbehörde zu genehmigen und zu überwachen wären. Offen bleibt außerdem, ob sich die Regelung eher an jeden einzelnen öffentlich-rechtlichen oder privaten Rundfunkveranstalter oder die beteiligten öffentlich-rechtlichen bzw. privaten Rundfunkveranstalter als Teilgruppe oder sogar an die Rundfunkveranstalter insgesamt richtet. Und offen bleibt schließlich, wie das geforderte „transparente Verfahren" auszusehen hätte, auf dessen Grundlage ein Verhaltenskodex entstehen und sodann veröffentlicht werden soll, insbesondere also beispielsweise, ob und gegebenenfalls in welcher Weise dabei die Gremien zu beteiligen wären.

16 Sowohl das „Ob" als auch das „Wie" eines Verhaltenskodex' überlässt die Vorschrift also den Verantwortlichen. Da ich den öffentlich-rechtlichen Rundfunk, wie eingangs bereits angesprochen, gerade auch datenschutzrechtlich in einer besonderen Verantwortung sehe, würde ich es allerdings begrüßen, wenn die Rundfunkanstalten insoweit die Initiative ergriffen. Sie könnten mithilfe eines Verhaltenskodex beschreiben, wie sie ihrer hervorgehobenen datenschutzrechtlichen Verantwortung gerade auch im Bereich der journalistischen Datenverarbeitung Rechnung tragen.

bb) Europa

17 Das zurückliegende Jahr war geprägt von der Diskussion über die Folgen der am 25. Mai 2018 in Kraft getretenen **Europäischen Datenschutzgrundverordnung (DSGVO[7])**. Sie hat die Aufmerksamkeit für Datenschutzthemen signifikant erhöht. Dies hat selbst in EU-Mitgliedstaaten wie Deutschland, die bereits eine umfassende

[7] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679&qid=1580735952286

Datenschutzgesetzgebung und eine ausdifferenzierte Aufsichtsstruktur hatten, zu weitreichenden Veränderungen sowohl in Bezug auf die rechtliche Ausgestaltung als auch in der Umsetzungspraxis geführt.

18 Die DSGVO hat die Unabhängigkeit der Datenschutzaufsicht deutlich gestärkt. Das geht schon daraus hervor, dass die in Art. 52 DSGVO geforderte „völlige Unabhängigkeit" ansonsten nur noch wenigen anderen Institutionen der EU wie der Europäischen Kommission, der Europäischen Zentralbank und dem Europäischen Bürgerbeauftragten zugeschrieben wird. Die für eine solche Unabhängigkeit erforderlichen Gewährleistungen und Absicherungsmechanismen hatte der Europäische Gerichtshof (EuGH) schon in den Jahren 2010, 2012 und 2014 in drei Urteilen konkretisiert[8]. Sie liegen den Vorschriften der DSGVO und den darauf basierenden nationalen Ausgestaltungsgesetzen zugrunde. Seither hat auch Deutschland die Unabhängigkeit der Datenschutzaufsichtsbehörden nicht nur funktional – im Sinne einer organisatorischen Trennung von den zu beaufsichtigenden Einrichtungen -, sondern institutionell ausgestaltet. Dementsprechend ist etwa der Bundesbeauftragte für Datenschutz und Informationsfreiheit inzwischen eine Oberste Bundesbehörde mit eigener Etat- und Personalhoheit, deren Amtschef vom Bundestag gewählt und nicht mehr von der Bundesregierung bestellt wird, und die weder einer Rechts- noch gar Fachaufsicht unterliegt; entsprechendes gilt für die Landesbeauftragten. Welche Bedeutung die DSGVO diesem Status beimisst, zeigt sich auch daran, dass Art. 45 Abs. 2 DSGVO die Bestätigung eines „angemessenen Schutzniveaus" in einem (nicht der EU angehörenden) Drittstaat (s. dazu auch unten Rn. 43 f.) unter anderem von der Existenz einer unabhängigen Datenschutzaufsicht abhängig macht.

19 Der DSGVO liegt ein Leitbild zugrunde, das auf der „Vertikalen" von einem engen Zusammenspiel einer strukturell verselbstständigten Aufsicht mit ihrerseits unabhängigen internen Datenschutzbeauftragten, die vor Ort die Umsetzung der Datenschutzvorgaben überwachen, sowie auf der „Horizontalen" einer ebenso engen Zusammenarbeit aller Aufsichtsbehörden untereinander ausgeht. Das Hauptaugenmerk der DSGVO liegt dabei insoweit – ihrem Charakter als europäischem Regelwerk entsprechend – auf der zwischenstaatlichen Zusammenarbeit. Dazu dient insbesondere der Europäische Datenschutzausschuss, in dem gemäß § 17 Abs. 1 S. 1 BDSG der Bundesbeauftragte für Datenschutz und Informationsfreiheit die deutschen Datenschutzaufsichtsbehörden vertritt; seinen Stellvertreter wählt der Bundesrat für die Dauer von 5 Jahren aus den Aufsichtsbehörden der Länder. Eine unmittelbare oder auch nur mittelbare Beteiligung der sonstigen Datenschutzaufsichtsbehörden, etwa der Rundfunkdatenschutzbeauftragten, sieht § 17 BDSG nicht explizit vor. Der DSGVO sind dazu keine weitergehenden Vorgaben zu entnehmen. Das verwundert nicht, weil ein föderal und „genrespezifisch" ausdifferen-

[8] Urteile vom 9.3.2010 – C 518/07 -, 16.10.2012 – C 614/10 -, 8.4.2014 – C 288/12 -

ziertes Aufsichtssystem wie das deutsche in anderen EU-Mitgliedstaaten unbekannt ist (s. dazu in Bezug auf den Bereich des Rundfunks noch unten Rn. 146).

20 Eindeutig ist allerdings, dass die DSGVO auf ein einheitliches Verständnis der materiellen Datenschutzanforderungen und eine einheitliche Umsetzung der Datenschutzstandards in den EU-Mitgliedstaaten angelegt ist. Zudem differenziert die DSGVO nicht zwischen unterschiedlich kompetenten oder relevanten Aufsichtsbehörden: jede Behörde, die die Anforderungen des Art. 51 DSGVO erfüllt, ist nach der ratio des DSGVO in dieses System zu integrieren. Es darf daher durchaus bezweifelt werden, ob § 18 Abs. 1 S. 1 BDSG europarechtskonform ist, soweit er die Zusammenarbeit und den damit verbundenen Informationsaustausch gemäß Abs. 1 S. 3 ausdrücklich auf die „Aufsichtsbehörden des Bundes und der Länder" beschränkt, die die sogenannten „spezifischen" Aufsichtsbehörden gemäß Abs. 1 S. 4 lediglich beteiligen sollen, sofern sie „von der Angelegenheit betroffen sind". Zu ihnen gehören außer den Rundfunkdatenschutzbeauftragten beispielsweise auch die Datenschutzaufsichten der Kirchen.

21 Nach der Interpretation der staatlichen Aufsichtsbehörden[9] sollen sie im Sinne von § 18 Abs. 1 S. 4 BDSG nur von solchen Themen bzw. Vorgängen „betroffen" sein, die dem spezifischen Umfeld der besonderen Aufsichtsbehörden zuzuordnen sind – also etwa dem Rundfunk für die Rundfunkdatenschutzbeauftragten. Daher verwundert es wenig, dass eine solche Beteiligung bislang noch nicht stattgefunden hat. Dies entspricht allerdings weder der bereits angesprochenen ratio der DSGVO noch der Aufsichtsstruktur. Denn jedenfalls dort, wo im (öffentlich-rechtlichen, aber auch privaten) Rundfunk die Datenschutzaufsicht einem Rundfunk- bzw. Mediendatenschutzbeauftragten übertragen wurde, erstreckt sich dessen Zuständigkeit auch auf die jeweiligen Beteiligungsgesellschaften und damit den privatrechtlichen Bereich.

22 Strukturell bestehen insoweit demzufolge keinerlei Unterschiede zu den staatlichen Aufsichtsbehörden, die eine Differenzierung unter dem Gesichtspunkt einer unterschiedlichen „Betroffenheit" rechtfertigen könnten. Daher sind die staatlichen Aufsichtsbehörden verpflichtet, die Rundfunkdatenschutzbeauftragten in verlässlicher, strukturierter Form in die Arbeit des europäischen Datenschutzausschusses einzubeziehen. Insbesondere genügt es dafür nicht, die Rundfunkdatenschutzbeauftragten allenfalls ex post von den Diskussionen oder Ergebnissen des Ausschusses zu informieren.

9 S. dazu den Beschluss der DSK vom 12.8.2019, https://www.datenschutzkonferenz-online.de/media/dskb/20190812_dsk_spezifische.pdf

23 Neben der DSGVO regelt die **VO (EU) 2018/1725**[10] den Datenschutz auf der Ebene der Europäischen Union, also in Bezug auf die Institutionen der EU selbst. Die inhaltlichen Vorgaben entsprechen naturgemäß denen der DSGVO. Die Aufsicht übertragen die Artt. 52 ff. einem gemeinsam durch das Parlament und den Rat der EU zu benennenden Europäischen Datenschutzbeauftragten, der auch den Vorsitz des Europäischen Datenschutzausschusses innehat. Selbstverständlich ist seine Funktion ebenfalls völlig unabhängig ausgestaltet.

24 Parallel zur DSGVO wollte die EU-Kommission die bisherige **E-Privacy-Richtlinie** (2002/58/EG[11]) ebenfalls durch eine EU-Verordnung ablösen, die – anders als eine Richtlinie – in den Mitgliedstaaten unmittelbar gilt. Dieses Vorhaben hat sie allerdings trotz mehrerer Anläufe bisher nicht umsetzen können. Bis auf weiteres verdrängen daher noch die spezifischeren Vorschriften der E-Privacy-Richtlinie die Regelungen der DSGVO, soweit sie vergleichbare Regelungsziele verfolgen und in nationales Recht umgesetzt worden sind. Nach ihrem Art. 3 richtet sich die E-Privacy-Richtlinie in erster Linie an Anbieter von Telekommunikationsdiensten (im Sinne des Telekommunikationsgesetzes) sowie teilweise an Anbieter von Telemedien (im Sinne des Telemediengesetzes). Für die Rundfunkanstalten und ihre Beteiligungsgesellschaften ist dies vor allem insoweit relevant, als es um den Einsatz sogenannter Cookies zur Erfassung von Nutzungsdaten in ihren Onlineangeboten geht. Hierzu enthält § 15 TMG spezifische Vorschriften. Angesichts der jüngeren Rechtsprechung des EuGH ist allerdings fraglich, ob sie mit den Vorgaben der E-Privacy-Richtlinie vereinbar und daher maßgeblich sind (s. dazu auch unten Rn. 59).

25 Außerdem ist noch auf die Ende 2018 aktualisierte, sogenannte **AVMD-Richtlinie in der Fassung der Richtlinie 2018/1808**[12] hinzuweisen. Einige dort neu eingefügte Vorschriften beschränken ausdrücklich das Recht der Verantwortlichen zur Verarbeitung personenbezogener Daten von Minderjährigen. So dürfen nach Art. 6a Abs. 2 sowie Art. 28b Abs. 3 AVMD-RiLi Mediendienste- bzw. Video-Sharing-Plattform-Anbieter die von Minderjährigen erhobenen oder anderweitig gewonnenen personenbezogenen Daten weder für kommerzielle Zwecke wie etwa Direktwerbung oder Profiling noch für Werbung verwenden, die auf das Nutzungsverhalten abgestimmt ist. Diese Vorgaben einschließlich der damit verbundenen Aufsichtszuständigkeiten sind bis spätestens 19. September 2020 in nationales Recht umzusetzen.

26 Mittelbar datenschutzrechtlichen Bezug hat schließlich die im November 2019 in Kraft getretene und bis 17. Dezember 2021 in nationales Recht umzusetzende Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23.

[10] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32018R1725&qid=1580735752304
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32002L0058&qid=1580735840113
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1580735678690&uri=CELEX:32018L1808

Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (**Whistleblower-Richtlinie)** [13]. Nach Erwägungsgrund (EG) 14 liegt ein erklärtes Ziel dieser Richtlinie unter anderem darin, auch Verstöße gegen die Achtung der Privatsphäre und den Schutz personenbezogener Daten, die als Grundrechte in den Artikeln 7 und 8 der EU-Grundrechtecharta (GRCh) verankert sind, aufzudecken und Hinweisgeber zu schützen. Diese könnten außerdem dazu beitragen, Verstöße von Anbietern wichtiger struktureller Dienste wie etwa von Cloud-Anwendungen gegen die ihnen obliegenden Verpflichtungen, etwa zur Meldung von Sicherheitsvorfällen oder sonstige Datenschutzvorschriften, aufzudecken.

27 Vom Anwendungsbereich der Richtlinie erfasst sind gemäß Art. 2 Abs. 1a) unter anderem Verstöße im Bereich des „öffentlichen Auftragswesens" (i) und gegen den Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen" (x), sowie gemäß Abs. 1c) Verstöße gegen Unionsvorschriften über Wettbewerb und staatliche Beihilfen. Die dem Anwendungsbereich der Richtlinie unterfallenden juristischen Personen des privaten und öffentlichen Rechts sind nach Art. 8 gehalten, „interne Meldekanäle" einzurichten, die ein geschütztes Hinweisgebersystem ermöglichen. Nach Erwägungsgrund 58 kann auch einem internen Datenschutzbeauftragten diese Aufgabe übertragen werden. Art. 18 enthält konkrete Vorgaben zur Dokumentation und Löschung der dabei anfallenden personenbezogenen Daten.

cc) Deutschland

28 Obwohl die DSGVO bereits seit Mai 2016 in Kraft getreten ist und seit 28. Mai 2018 unmittelbar in allen Mitgliedstaaten gilt, war auch noch das Jahr 2019 in Deutschland von umfangreichen gesetzgeberischen Anpassungs- und Umsetzungsmaßnahmen gekennzeichnet. Erst am 26. November 2019 trat das 2. Datenschutz-Anpassungsgesetz in Kraft[14], auf dessen Grundlage rund 150 spezielle Bundesgesetze an die durch die DSGVO veränderte Rechtslage angepasst wurden.

29 Dazu zählte nicht zuletzt das **Deutsche Welle-Gesetz**, das jetzt in der Fassung vom 20.11.2019 gilt[15]. Es enthält nun alle für die Deutsche Welle maßgeblichen Datenschutzregelungen. Leider hat der Bundesgesetzgeber bei dieser Gelegenheit die Zuständigkeit für die Datenschutzaufsicht über die Datenverarbeitung der DW geteilt: Nach § 65 Abs. 1 beaufsichtigt der – jetzt so genannte – Beauftragte für den Datenschutz der Deutschen Welle die Einhaltung der Datenschutzvorschriften, soweit die DW oder ein Hilfsunternehmen personenbezogene Daten zu journalistischen Zwecken verarbeitet. Insoweit überträgt S. 2 dem Beauftragten für den Da-

[13] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019L1937
[14] Übersicht und vollständiger Überblick: http://dipbt.bundestag.de/extrakt/ba/WP19/2390/239070.html
[15] http://www.gesetze-im-internet.de/dwg/DWG.pdf

tenschutz, der dieses Amt gemäß § 64 Abs. 5 grundsätzlich auch neben anderen Aufgaben ausüben darf, ausdrücklich die Aufgaben und Befugnisse gemäß Art. 57 und 58 Abs. 1 bis 5 DSGVO. Im übrigen - also jenseits der (wenngleich ausweislich der amtlichen Begründung weit auszulegenden) journalistischen Datenverarbeitung - obliegt gemäß § 65 Abs. 1 S. 3 allerdings die Aufsicht über die Einhaltung von Datenschutzbestimmungen jetzt dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

30 Damit folgt der Bundesgesetzgeber einem Modell der „gespaltenen" Aufsicht, das seit längerem bereits in Berlin/Brandenburg (für den Rundfunk Berlin-Brandenburg), Bremen (Radio Bremen) und Hessen (Hessischer Rundfunk) gilt. Dem Gebot der staatsfernen Organisation des öffentlich-rechtlichen Rundfunks entspricht es erkennbar weniger als die für alle anderen Rundfunkanstalten eingerichtete, vollständig autonome Datenschutzaufsicht. Zwar sind auch die Datenschutzaufsichtsbehörden des Bundes und der Länder infolge der ihrerseits garantierten völligen Unabhängigkeit nicht unmittelbar anderen staatlichen Institutionen gleichzusetzen. Wohl aber sind sie institutionell und funktional der Staatsorganisation zuzuordnen, der der öffentlich-rechtliche Rundfunk in Deutschland aus gutem Grund nicht angehört. Außerdem kann die Abgrenzung zwischen einer Datenverarbeitung zu journalistischen und einer solchen zu „anderen" Zwecken angesichts der sich immer mehr auflösenden Grenzen beispielsweise im Bereich Medienproduktion, -ausspiel und -layout zu großen Schwierigkeiten und zu unnötigem Kompetenzklärungsaufwand führen.

31 Möglicherweise hat sich der Bundesgesetzgeber daran gehindert gesehen, für eine Bundeseinrichtung wie die DW von der Ermächtigung des Art. 85 Abs. 2 DSGVO so weitgehend Gebrauch zu machen wie die Länder, weil er seine Gesetzgebungskompetenz anders als diese hinsichtlich dieser Rundfunkanstalt nicht auf die (dem Einfluss der EU entzogene) Ausgestaltung der Rundfunkorganisation gemäß Art. 5 Abs. 1 S. 2 GG, sondern „nur" auf Art. 73 Abs. 1 Nr. 1 GG („auswärtige Angelegenheiten") stützen kann. Im Interesse einer einheitlichen Konstruktion der Datenschutzaufsicht im deutschen öffentlich-rechtlichen Rundfunk wäre es jedoch wünschenswert gewesen, wenn der Bund etwaige dahingehende Bedenken zurückgestellt und das (geringe) Risiko einer möglichen Auseinandersetzung mit der Kommission dazu in Kauf genommen hätte.

32 Neben dem Beauftragten für den Datenschutz sieht § 66 DW-Gesetz auch weiterhin ausdrücklich die Bestellung eines internen Datenschutzbeauftragten gemäß §§ 5 – 7 BDSG vor. Eine entsprechende Verpflichtung hätte sich ansonsten im Zweifel ohnehin aus Art. 37 Abs. 1a) DSGVO ergeben, da die DW als „öffentliche Stelle" im Sinne dieser Vorschrift anzusehen sein dürfte.

33 Im Zuge des 2. DSAnpG ist im übrigen nach längerer Auseinandersetzung und gegen den Widerstand der staatlichen Datenschutzaufsichtsbehörden die Relevanzschwelle angehoben worden, oberhalb derer nach § 38 Abs. 1 BDSG „nichtöffentliche Stellen" – also privatrechtliche Unternehmen bzw. Einrichtungen – einen **Datenschutzbeauftragten** zu benennen haben[16]. Dies ist seither nur noch dann erforderlich, wenn sie in der Regel mindestens zwanzig (und nicht mehr nur zehn) Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Diese Anpassung ist im Kontext des vielfach erhobenen Vorwurfs zu sehen, die DSGVO differenziere ihre Anforderungen nicht hinreichend zwischen internationalen Konzernen und kleineren Unternehmen, die deshalb unzumutbar belastet würden. Diese Frage dürfte auch im Mittelpunkt der im Mai 2020 erstmals anstehenden Evaluation der DSGVO stehen, Art. 97 DSGVO.

34 Abschließend ist noch auf zwei Gesetzesvorhaben des Bundesministeriums des Innern, für Bau und Heimat hinzuweisen, die im Jahr 2019 noch nicht abgeschlossen worden sind. In beiden Fällen beförderten Recherchen des Onlineportals „netzpolitik.org" die entsprechenden Entwürfe an die Öffentlichkeit, die aus unterschiedlichen Gründen je für sich aus der Sicht des öffentlich-rechtlichen Rundfunks bzw. seiner Datenschutzaufsicht ganz grundsätzliche Fragen aufwerfen:

35 Zum einen geht es um eine **Novellierung des BSI-Gesetzes**[17]. Sie verfolgt das Ziel, den Schutz vor und die Abwehr von Cyber-Angriffen bzw. die Reaktion darauf zu verbessern und insoweit insbesondere die Befugnisse des Bundesamts für Informationssicherheit (BSI) erheblich zu erweitern. Im entsprechenden Referentenentwurf vom 27. März 2019[18] ist dazu unter anderem die Ergänzung des § 2 um einen neuen Absatz 14 vorgesehen, der künftig als „Infrastrukturen im besonderen öffentlichen Interesse" (KRITIS) auch solche „Anlagen oder Teile davon" qualifizieren soll, „die dem Bereich Kultur und Medien angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung eine Gefährdungen für die öffentliche Sicherheit eintreten würde."

36 Sowohl nach ihrem Wortlaut als auch ihrer ratio würden einer solchen Vorschrift aus dem Medienbereich im Zweifel in erster Linie die IT-Infrastrukturen der Rundfunkanstalten subsumiert werden können. Denn sowohl nach Maßgabe ihres verfassungsrechtlichen Funktionsauftrags als auch der für sie jeweils geltenden gesetzlichen oder staatsvertraglichen Verpflichtungen sollen die Rundfunkanstalten die Information der Bevölkerung gerade im Krisenfall – insbesondere durch Verbreitung amtlicher Verlautbarungen - zuverlässig gewährleisten (vgl. bspw. § 10

16 http://www.gesetze-im-internet.de/bdsg_2018/__38.html
17 https://www.gesetze-im-internet.de/bsig_2009/
18 https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/

ZDF- bzw. Deutschlandradio-Staatsvertrag). Diese spezifische Obliegenheit dürfte für sich genommen auch unter den heutigen Bedingungen der elektronischen Massenkommunikation verfassungsrechtlich vertretbar sein. Insofern verweist die Begründung des Referentenentwurfs grundsätzlich durchaus zu recht auf die Gefahren, die Cyberangriffe auf Medien „für die Gesellschaft und die Regierung" sowie „die freiheitlich demokratische Grundordnung der Bundesrepublik" haben.

37 Eine ganz andere Frage ist indessen, ob dieser Befund den Bund berechtigt, den öffentlich-rechtlichen Rundfunk (bzw. die von ihm genutzte IT-Infrastruktur) spezifischen Anforderungen und letztlich auch umfangreichen Zu- und Eingriffsbefugnissen des BSI zu unterwerfen. Denn eben dies wäre mit der Einordnung als „KRITIS-Segment" verbunden. So wären sie etwa nach dem ebenfalls neu einzufügenden § 8a Abs. 1a) BSI-Gesetz als Betreiber Kritischer Infrastrukturen verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit dieser Strukturen maßgeblich sind, darunter auch den Einsatz von Systemen zur Angriffserkennung (s. dazu auch unten Rn. 160 ff.). Über die entsprechenden Verfahren und Umstände solcher Maßnahmen müssten sie nach S. 4 dieser neuen Vorschrift „der oder dem betrieblichen Datenschutzbeauftragten, dem Bundesamt, der jeweiligen Aufsichtsbehörde und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert schriftlich berichten." Der Entwurf der amtlichen Begründung zu dieser Neuregelung taxiert den allein durch diese Neuregelung ausgelösten personellen Zusatzbedarf des BSI auf sage und schreibe 56 Planstellen. Der organisatorische und personelle Aufwand in den Rundfunkanstalten – die ohnedies nicht unter dem Mangel an gesetzlich vorgegebenem Berichtswesen leiden - wäre gewiss ebenfalls erheblich.

38 Eine weitere gesetzgeberische Aktivität, die in datenschutzrechtlicher Hinsicht in Bezug auf ihre potentiellen Auswirkungen insbesondere auf den Medienbereich als gelinde gesagt problematisch zu bewerten ist, ist der Ende März 2019 bekannt gewordene **Entwurf** eines „**Gesetzes zur Harmonisierung des Verfassungsschutzrechts**"[19]. Dieses soll den Inlands- und Auslandsgeheimdiensten einen weitgehenden Zugriff auf „informationstechnische Systeme" etwa von sogenannten Gefährdern, aber auch Anbietern von Internet-Diensten, derer sich Gefährder bedienen, ermöglichen. Mithilfe eines sogenannten „Staatstrojaners" wäre dann auch die Online-Durchsuchung von Servern, Computern, Smartphones und sonstigen Geräten von Rundfunkanstalten, Verlagen sowie deren Journalisten möglich. Dass dies das streng und ansonsten umfassend geschützte Redaktionsgeheimnis unter-

[19] https://netzpolitik.org/2019/wir-veroeffentlichen-den-gesetzentwurf-seehofer-will-staatstrojaner-fuer-den-verfassungsschutz/

laufen bzw. aushöhlen würde, liegt auf der Hand[20]. Dementsprechend ist einer derart weitgehenden Ermächtigung zu geheimdienstlicher Datenerhebung bei allem Verständnis für die gestiegene Bedrohungslage durch Cyber- und sonstige Kriminalität auch und gerade aus Sicht der rundfunkspezifischen Datenschutzaufsicht mit allem Nachdruck zu widersprechen.

dd) Länder

39 Zuständig für die Regulierung von Rundfunk und rundfunkähnlichen Telemedien sowie die Presse sind in Deutschland grundsätzlich die Bundesländer. Das gilt auch, soweit es um die Datenschutzaufsicht über die Anbieter solcher Medien geht (siehe § 9c Abs. 4 RStV). Es läge nahe, die entsprechenden Strukturen zumindest für den öffentlich-rechtlichen Rundfunk länderübergreifend zu vereinheitlichen. Dies würde allerdings eine entsprechende staatsvertragliche Rahmengesetzgebung voraussetzen. Da es zu einer solchen bislang nicht gekommen ist, unterscheidet sich die Ausgestaltung im Detail. Insbesondere sind mit dem Hessischen Rundfunk, Radio Bremen und Rundfunk Berlin-Brandenburg drei Landesrundfunkanstalten von dem von ihren Bundesländern eingeschlagenen Sonderweg einer „gespaltenen" Aufsichtszuständigkeit (s. bereits oben Rn. 29 f. zur DW) betroffen. Noch unterschiedlicher fallen die Aufsichtsregelungen für den privaten Rundfunk sowie die Telemedienanbieter aus. Die konkreten Einzelheiten ergeben sich aus dem jeweiligen Landesmedien-, Landesrundfunk- oder Landesdatenschutzgesetz (dazu unten Rn. 102 f.).

40 In Bezug auf die meiner Aufsicht unterliegenden fünf Rundfunkanstalten haben die jeweils zuständigen Länder die einschlägigen Vorgaben der DSGVO mit Wirkung zum 25. Mai 2018 staatsvertraglich bzw. gesetzlich weitestgehend gleichlautend und umfassend umgesetzt. Geringfügige Abweichungen ergeben sich etwa für die Amtszeit des Rundfunkdatenschutzbeauftragten (im Regelfall vier, für den Saarländischen Rundfunk sechs Jahre) oder die Vorgaben zum Tätigkeitsbericht (s. bereits oben Rn. 1 f.).

41 Im Oktober 2019 unterzeichneten die Regierungschefinnen und Regierungschefs der Länder den 23. Rundfunkänderungsstaatsvertrag mit einer **Neufassung des Rundfunkbeitragsstaatsvertrags**, die – nach der Ratifizierung durch alle Landtage – zum 1. Juni 2020 in Kraft treten soll[21]. Sie enthält neben den durch die Ent-

[20] Siehe auch https://netzpolitik.org/2019/reporter-ohne-grenzen-warnt-vor-aushoehlung-des-redaktionsgeheimnisses/

[21] https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/23._Staatsvertrag_zur_AEnderung_rundfunkrechtlicher_Staatsvertraege_als_pdf-Datei.pdf

scheidung des Bundesverfassungsgerichts vom 18. Juli 2018 erforderlich gewordenen Vorgaben zur Befreiung von Zweitwohnungen von der Beitragspflicht in § 11 Abs. 5 S. 1 unter anderem eine Neuregelung zum Meldedatenabgleich, zu den Löschungsverpflichtungen des Beitragsservice (§ 11 Abs. 5 S. 2), und zu Auskunftsansprüche der Betroffenen gegen die Landesrundfunkanstalten bzw. den Beitragsservice (§ 11 Abs. 8) sowie eine Neufassung des Zweckbindungsgrundsatzes (§ 11 Abs. 9). Gegen die Einführung des regelmäßigen vollständigen Meldedatenabgleichs hatte sich im Vorfeld die Konferenz der staatlichen Datenschutzaufsichtsbehörden ausgesprochen[22]. Den dort insbesondere unter Hinweis auf die unterstellte Unverhältnismäßigkeit dieses Mittels geltend gemachten verfassungs- und datenschutzrechtlichen Bedenken schlossen sich die Länder allerdings – aus meiner Sicht zu recht - nicht an.

b Datenschutzrelevante Entwicklungen

aa) Internationaler Datenverkehr

42 Die Rundfunkanstalten oder ihre Beteiligungsunternehmen übertragen personenbezogene Daten auch in Staaten, die nicht der EU angehören. Eine solche Datenübermittlung ist beispielsweise mit dem Einsatz von Produkten US-amerikanischer Konzerne wie Microsoft, IBM, Amazon (der mit AWS das weltweit führende Cloud-System anbietet) oder Google verbunden. Art. 44 DSGVO erklärt eine solche Datenübermittlung allerdings grundsätzlich nur für zulässig, wenn die Verantwortlichen in einem solchen sogenannten Drittland ihrerseits die Vorgaben der DSGVO einhalten. Mittelbar entfaltet die DSGVO daher eine Wirkung, die weit über ihren direkten Geltungsbereich hinausgeht.

43 Indessen wären die Verantwortlichen mit einer Prüfung, ob Drittstaaten ein der DSGVO entsprechendes Schutzniveau vorsehen, im Zweifel überfordert; zudem wäre auf dieser Basis das von der DSGVO angestrebte einheitliche Verständnis aller datenschutzrechtlichen Rahmenbedingungen nicht herstellbar. Daher sieht Art. 45 DSGVO eine entsprechende Prüfung durch die EU-Kommission vor, deren Ergebnis ein sogenannter Angemessenheitsbeschluss sein kann. Eine darauf gestützte Datenübermittlung an ein Drittland bedarf gem. Art. 45 Abs. 1 S. 2 DSGVO keiner besonderen Genehmigung. Falls ein solcher Beschluss nicht vorliegt, macht Art. 46 DSGVO die Übermittlung personenbezogener Daten an ein Drittland davon abhängig, dass die Standards der DSGVO durch anderweitige geeignete Garantien abgesichert sind und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Dazu können unter anderem von der

[22] https://www.datenschutzkonferenz-online.de/media/dskb/20190426_dsk-beschluss_rfbeitrag.pdf

Kommission genehmigte Standarddatenschutzklauseln gehören, Art. 46 Abs. 2 DSGVO. Das außerdem erforderliche Einverständnis der Vertragspartner ist den US-amerikanischen Großkonzernen freilich im Regelfall nicht abzuringen. Ausnahmen von diesen Vorgaben sieht Art. 49 DSGVO nur für bestimmte Fälle und unter engen Voraussetzungen vor.

44 Bislang hat die Kommission etwa ein Dutzend Angemessenheitsentscheidungen veröffentlicht[23]. Mit Abstand die größte Bedeutung hat insoweit das Verhältnis zu den **USA**. Den ursprünglichen Beschluss der Kommission, die Datenübermittlung auf der Grundlage des sogenannten „Safe-Harbour"-Abkommens mit dem US-Handelsministerium für angemessen zu erklären, hat der EuGH bereits im Oktober 2015 für ungültig erklärt[24]. Auch das anschließend stattdessen geschlossene Abkommen zum US-Privacy-Shield bzw. der darauf bezogene Angemessenheitsbeschluss der Kommission ist bereits Gegenstand eines Verfahrens vor dem EuGH, mit dessen Abschluss im Jahr 2020 zu rechnen ist. Die Zweifel an der Vergleichbarkeit des Datenschutzniveaus in den USA mit den Standards der DSGVO beziehen sich auch auf den im März 2018 in Kraft getretenen sogenannten CLOUD (Clarifying Lawful Overseas Using of Data)-Act, der US-amerikanische Unternehmen verpflichtet, den dortigen Behörden unabhängig davon einen Datenzugriff zu ermöglichen, wo die Speicherung stattfindet. Weitergehende datenschutzrechtliche Anforderungen als in den USA sonst üblich enthält bislang lediglich der zum 1. Januar 2020 in Kraft getretene California Consumer Privacy Act (CCPA), der zwar primär das Ziel des Verbraucherschutzes verfolgt, aber zahlreiche Garantien der DSGVO übernommen hat.

45 Vor diesem Hintergrund ist die Inanspruchnahme von Dienstleistungen der großen US-amerikanischen Konzerne, insbesondere soweit es um Büroanwendungen und IT-Infrastrukturen wie etwa die Nutzung von Cloud-Speicherung geht (s. dazu auch unten Rn. 169), unverändert mit erheblichen Risiken in Bezug auf die Gewährleistungen von Datenschutz und Datensicherheit verbunden. Mindestens ebenso gewichtig sind die strategischen Konsequenzen einer zunehmenden Abhängigkeit von den betreffenden Anbietern[25]. Selbstverständlich stehen vor diesem Problem nicht nur die Verantwortlichen in meinem Zuständigkeitsbereich, sondern es betrifft alle Anwender in der EU. Dies enthebt sie allerdings nicht von der Verpflichtung, sich mit allen damit verbundenen Gefahren insbesondere für die Informationssicherheit

23 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de

24 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:62014CJ0362

25 Aufschlussreich dazu mit Blick auf die Bundesbehörden die im Auftrag des BMI entstandene Studie „Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern" vom August 2019, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.html?nn=4623908

gründlich zu befassen, die für sie jeweils maßgeblichen Gesichtspunkte zu bewerten und die Gründe für ihre Entscheidung zu dokumentieren, Art. 5 Abs. 2 DSGVO.

46 Zwei weitere Drittstaaten seien in diesem Zusammenhang noch erwähnt, die im Wirtschafts- bzw. Datenverkehr zunehmend bedeutsam werden: Zum einen **China**, dessen IT- und Telekommunikationsindustrie in den letzten Jahren erheblich an Marktanteilen und Einfluss gewonnen hat. Seit mit „TikTok" auch im Bereich der sogenannten „Sozialen Netzwerke" ein chinesisches Unternehmen tätig ist, dessen in Europa zunehmend genutztes Angebot sich zudem vornehmlich an die in datenschutzrechtlicher Hinsicht besonders schutzwürdigen Minderjährigen richtet, wird in der Öffentlichkeit verstärkt die Frage des Datenschutzes im Verhältnis zu diesem Land diskutiert. Mit einem Angemessenheitsbeschluss der Kommission ist hier angesichts der bislang bekannt gewordenen Diskrepanz zwischen der exzessiven Datennutzungs- und Überwachungspraxis in China und den Standards der DSGVO in absehbarer Zeit nicht zu rechnen.

47 Ein Angemessenheitsbeschluss fehlt auch noch im Verhältnis zum bisherigen EU-Mitglied **Großbritannien**, das die EU am 31. Januar 2020 verlassen hat. Mit Blick auf die noch bis Ende des Jahres 2020 verabredete Übergangsfrist bleibt abzuwarten, ob ein derartiger Beschluss Teil des „geregelten Brexit" sein wird. Falls es dazu nicht kommt, müsste sich die EU-Kommission gesondert mit dem Thema befassen.

bb) Rechtsprechung auf europäischer Ebene

48 Zunehmend beeinflusst die Rechtsprechung des **Europäischen Gerichtshofs** (EuGH) das europäische und damit auch nationale Datenschutzrecht. Auch im Jahr 2019 hat er eine ganze Reihe grundsätzlicher Entscheidungen veröffentlicht, von denen hier die mit unmittelbarem oder mittelbarem Bezug zum Datenschutz im Rundfunkbereich kurz dargestellt seien:

49 Im Verfahren C-345/17 ging es darum, dass eine Privatperson in Lettland ihre Vernehmung in einer Polizeidienststelle sowie die Aktivitäten der Polizisten dort heimlich gefilmt und die Aufnahmen anschließend auf YouTube veröffentlicht hatte. Die lettische Datenschutzaufsicht ordnete daraufhin die Löschung des YouTube-Videos an, gegen die sich der Kläger wandte. In seinem **Urteil vom 14.02. 2019**[26] stellte der EuGH fest, dass es auch in einem solchen Fall um eine „Datenverarbeitung allein zu journalistischen Zwecken" gehen kann. Seine datenschutzrechtliche Bewertung bezog sich zwar noch auf die einschlägige Vorschrift der

[26] http://curia.europa.eu/juris/document/document.jsf?text=&docid=210766&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=4227775

durch die DSGVO abgelösten Datenschutzrichtlinie, dürfte aber ohne weiteres auch für die Auslegung von Art. 85 DSGVO maßgeblich sein. Im Kern geht es dabei um die Reichweite der Garantien zur Informations- und Meinungsfreiheit im Verhältnis zum Schutz des Persönlichkeitsrechts und damit den Anwendungsbereich des sog. Medienprivilegs (s. dazu bereits Rn. 4 ff. und unten Rn. 195 ff.). Die Feststellung, ob es um eine Aktivität geht, die dazu dienen soll, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten, ist ebenso Sache der jeweils zuständigen Gerichte wie die Beurteilung, ob die jeweils einschlägigen gesetzlichen Vorkehrungen sich gemessen an dem Veröffentlichungsgegenstand auf das zum Schutz der Privatsphäre absolut Notwendige beschränken (Urteil Rn. 66, 68).

50 Auf große Resonanz stieß das **Urteil vom 29.7.2019** (C 40/17) zum „Facebook-Like-Button“[27]. Auslöser war in diesem Fall ein von einer Verbraucherschutzorganisation eingeleitetes Verfahren gegen einen Online-Händler für Modeartikel (Fashion ID). Dieser setzte auf seiner Website ein sogenanntes Plugin in Gestalt des „Gefällt mir“-Buttons ein, mit dem über den US-amerikanischen Plattformanbieter Facebook das eigene Onlineangebot bewertet und weiter kommuniziert werden kann. Technisch handelt es sich um eine Verknüpfung des eigenen Angebots mit dem eines Dritten. Will der Betreiber einer Website derartige Drittinhalte einbinden, setzt er auf dieser Website einen Verweis auf den externen Inhalt. Stößt der Browser des Besuchers auf diesen Verweis, fordert er den Inhalt von dem Drittanbieter an und fügt ihn an der gewünschten Stelle in die Darstellung der Website ein. Hierzu übermittelt der Browser dem Server des Drittanbieters die IP-Adresse des Rechners dieses Besuchers sowie die technischen Informationen des Browsers, damit der Server feststellen kann, in welchem Format der Inhalt an welche Adresse auszuliefern ist. Daneben übermittelt der Browser auch Informationen zu dem gewünschten Inhalt. Welche Informationen der Browser übermittelt und was der Drittanbieter mit diesen Informationen macht, insbesondere, ob er diese speichert und auswertet, kann der Betreiber, der den Drittinhalt auf seiner Website einbindet, nicht beeinflussen.

51 Im Verfahren vor dem EuGH ging es um die Frage, ob und inwieweit das Unternehmen, das sein Angebot durch das Einbinden des „Like-Buttons“ mit Facebook verknüpft, auch für die auf der dortigen Plattform stattfindende bzw. ermöglichte Datenverarbeitung verantwortlich ist. Dies hat der EuGH grundsätzlich bejaht. Diese Verantwortung sei allerdings auf die Vorgänge beschränkt, für die der Betreffende tatsächlich über die Zwecke und Mittel der Datenverarbeitung entscheide, im betreffenden Fall also das Erheben der Daten (auf der eigenen Website) und deren Übermittlung an Facebook. Der Sache nach seien also beide beteiligten Unternehmen – wenn auch in unterschiedlicher Weise – für die durch das Einbinden des

[27] http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=4229041

Plugins ausgelöste Datenverarbeitung verantwortlich. Eine solche gemeinsame Verantwortlichkeit setze nicht voraus, dass jeder Beteiligte Zugang zu den betreffenden personenbezogenen Daten habe (Urteil Rn. 68 f.). Der gemeinsamen Verantwortung korrespondierten in einem solchen Fall die jeweiligen Informationspflichten und die Pflicht, die erforderliche Einwilligung einzuholen (Urteil Rn. 98 ff.).

52 Da die Verantwortlichen in meinem Zuständigkeitsbereich in vielfältiger Weise auf die Angebote von Facebook (und ähnlicher Plattformen) zurückgreifen, ist das Urteil auch für sie bedeutsam (s. dazu auch unten Rn. 170 ff.).

53 In zwei weiteren Verfahren (C 136/17 und C 507/17) befasste sich der EuGH mit der datenschutzrechtlichen Einordnung und Bewertung von Suchmaschinen – hier: jeweils Google - und deren Auswirkungen auf den Schutz personenbezogener Daten. Google hatte sich geweigert, verschiedene Links auf mehrere Personen, die in der Vergangenheit aus unterschiedlichen Anlässen Gegenstand von Veröffentlichungen gewesen waren, aus den automatisch generierten Trefferlisten zu entfernen bzw. die Anzeige zu unterbinden. Die französische Datenschutzaufsichtsbehörde war auf die Beschwerde der Petenten hin nicht gegenüber Google tätig geworden. Mit seinen **Urteilen vom 24.9.2019** stellte der EuGH fest, dass das Verbot bzw. die Beschränkungen der hier maßgeblichen Datenschutzrichtlinie zur Verarbeitung besonderer Kategorien personenbezogener Daten auch auf einen Suchmaschinenbetreiber anwendbar sind. Dieser hat deshalb grundsätzlich dahingehenden Anträgen auf Auslistung von Links zu Websites stattzugeben, sofern die Veröffentlichung nicht auf eine der Ausnahmeregelungen gestützt werden kann und keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen. Daher habe der Suchmaschinenbetreiber in einem solchen Fall mit Blick auf die durch Art. 17 Abs. 3 DSGVO geforderte Abwägung zwischen den in den Art. 7 und 8 der EU-Grundrechtecharta verankerten Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten und dem durch Art. 11 der Charta gewährleisteten Grundrecht auf freie Information alle maßgeblichen Belange zu berücksichtigen und seiner Entscheidung zugrunde zu legen (Urteil C 136/17 Rn. 56 ff.)[28].

54 In der Parallelsache C 507/17[29] stellte der EuGH allerdings klar, dass sich dieses „Recht auf Vergessenwerden“ (so die Bezeichnung in Art. 17 DSGVO) nur auf die mitgliedstaatlichen Versionen der Suchmaschinen beschränkt.

[28] http://curia.europa.eu/juris/document/document.jsf?text=&docid=218106&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=4233591

[29] http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=4240251

55 Für einige Aufregung sorgte der EuGH mit seinem **Urteil vom 1.10.2019** in der Sache C-673/17[30]. Auslöser war ein Vorlagebeschluss des BGH zum Verständnis der für die Wirksamkeit einer Einwilligung maßgeblichen europäischen Datenschutzvorschriften, namentlich von Art. 6 Abs. 1 lit. a) DSGVO. Im vorliegenden Fall ging es dabei um die Erhebung personenbezogener Daten über sogenannte Cookies. Ein deutscher Onlineanbieter hatte auf seiner Website ein Gewinnspiel veranstaltet, an dem teilnehmen konnte, wer seine Postleitzahl in ein entsprechendes Feld eingab. Daraufhin wurde eine Internetseite mit weiteren Eingabefeldern für Namen und Adresse angezeigt. Unter den Eingabefeldern für die Adresse befanden sich zwei mit Ankreuzkästchen versehene Hinweistexte. Eines dieser Kästchen war bereits mit einem voreingestellten Kreuz markiert; danach erklärte sich der Nutzer mit dem Einsatz eines Webanalysedienstes einverstanden, mit der Folge, dass der Gewinnspielveranstalter nach Registrierung für das Gewinnspiel Cookies setzen durfte, die eine Auswertung des Surf- und Nutzungsverhaltens auf Websites von Werbepartnern und damit interessengerichtete Werbung durch den Webanalysedienst ermöglichte. Ferner wies die Erklärung auf die Möglichkeit hin, die Cookies jederzeit wieder zu löschen.

56 Nach dem Urteil des EuGH ist eine solche Konstruktion nicht geeignet, eine wirksame Einwilligung einzuholen (Urteil Rn. 52 ff.). Denn erforderlich sei ein ohne jeden Zweifel nachweisbares aktives Verhalten („Opt-In"), das ein voreingestelltes Ankreuzkästchen („Opt-Out") gerade nicht evoziere. Da eine wirksame Einwilligung überdies nur auf der Grundlage einer umfassenden und verständlichen Information zustande komme, gehöre zu den dafür zwingend erforderlichen Informationen auch die Angabe über die Funktionsdauer der entsprechenden Cookies und zur etwaigen Möglichkeit Dritter, auf die dort verarbeiteten Daten zuzugreifen (Urteil Rn. 81). Soweit es dabei um die Auslegung der Vorschriften der ePrivacy-Richtlinie (hier: Art. 5 Abs. 3) gehe, erstrecke sich deren Schutz im übrigen auf sämtliche in einem Endgerät mithilfe von Cookies gespeicherte Informationen, unabhängig davon, ob es sich dabei um personenbezogene Daten handele, insbesondere also auch auf sogenannte „hidden identifiers" oder ähnliche Instrumente, die ohne das Wissen der Nutzer in deren Endgeräte eindringen (Urteil Rn. 70).

57 Nach Maßgabe der Auslegungsgrundsätze des EuGH hat nun der BGH den zugrunde liegenden Rechtsstreit zu entscheiden; mit seinem Urteil ist im Laufe des Jahres 2020 zu rechnen.

58 Große Bedeutung hat die Frage des zulässigen Einsatzes von Cookies für alle Formen der Nutzungsmessung, insbesondere für die Werbewirtschaft, aber auch für

[30] http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=4270553

die Rundfunkanstalten, die entsprechende Instrumente einsetzen, um die publizistische Wirksamkeit ihrer Onlineangebote zu optimieren. Entgegen dem zunächst entstandenen Eindruck lässt sich aus dem Urteil des EuGH nicht ableiten, dass nun alle einschlägigen Cookies nur noch mit Einwilligung der Betroffenen eingesetzt werden dürfen. Denn der EuGH hat sich in dem Verfahren nur mit der Frage der Anforderungen an eine wirksame Einwilligung als solche und nicht damit beschäftigt, in welchen Fällen der Verantwortliche tatsächlich eine Einwilligung benötigt oder sich ggf. auf eine andere Rechtsgrundlage berufen kann.

59 Allerdings lässt sich aus der Zusammenschau mit dem bereits erwähnten Urteil vom 29.7.2019 (oben Rn. 50 f.) zumindest eine Tendenz ableiten, nach der der EuGH im Zweifel jedenfalls für alle nicht technisch bzw. funktional „unbedingt erforderlichen" Cookies eine Einwilligung für nötig hält. Für das deutsche Recht ist dies jedoch (noch) nicht unmittelbar relevant, weil die Vorschrift des § 15 Abs. 3 TMG spezifische Erlaubnistatbestände enthält. Zwar sprechen gute Gründe dafür, dass diese Vorschrift nach der Rechtsprechung des EuGH mit den Vorgaben der ePrivacy-Richtlinie nicht (mehr) vereinbar ist[31]. Aber solange sie nicht für unwirksam erklärt worden ist, dürfen sich deutsche Anbieter grundsätzlich auf sie berufen. Den Rundfunkanstalten ist dazu allerdings, insbesondere mit Blick auf die Anwendbarkeit der in Art. 6 Abs. 1 DSGVO genannten Erlaubnistatbestände, ein besonders sorgsamer Umgang mit den von ihnen eingesetzten Cookies zu empfehlen (s. dazu unten Rn. 177 ff., 181 ff.).

60 Schließlich sei noch auf eine Entscheidung des EuGH mit arbeitsrechtlichem Bezug hingewiesen, die viele Arbeitgeber in Deutschland dazu zwingen wird, künftig in erheblich größerem Umfang als bisher personenbezogene Daten ihrer Beschäftigten zu verarbeiten. Denn mit seinem **Urteil vom 14. Mai 2019** (C-55/18)[32] stellte der EuGH fest, dass nur durch eine vollständige Erfassung der Arbeitszeiten die auf Art. 31 Abs. 2 EU-GRCh gestützten Vorgaben des europäischen Rechts etwa zur wöchentlichen Höchst- sowie zur täglichen oder wöchentlichen Mindestruhezeit objektiv überprüfbar und zuverlässig zu gewährleisten sei (Urt. Rn. 50 f.). Alle Mitgliedstaaten seien zu entsprechenden gesetzlichen Vorgaben verpflichtet.

61 Der in Deutschland unter dem Stichwort „Vertrauensarbeitszeit" weit verbreitete Verzicht auf umfassende Arbeitszeitnachweise (nicht hingegen notwendigerweise die Praxis der Vertrauensarbeitszeit als solche) ist unter diesen Vorzeichen nicht länger aufrechtzuerhalten. Dies gilt branchenübergreifend und damit auch für alle Arbeitgeber in meinem Zuständigkeitsbereich. Selbstverständlich ist die damit ver-

[31] Siehe dazu die „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien" vom März 2019, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

[32] http://curia.europa.eu/juris/document/document.jsf?text=&docid=214043&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=4278624

bundene umfangreiche Verarbeitung personenbezogener Daten aller Beschäftigten, insbesondere deren Erhebung, Speicherung und Auswertung nur nach Maßgabe der generellen Vorgaben der europäischen und nationalen Datenschutzgesetze sowie gegebenenfalls auch tariflicher oder betrieblicher Vereinbarungen zulässig.

cc) Deutschland

62 Neben dem EuGH hat sich auf nationaler Ebene auch das **Bundesverfassungsgericht** (BVerfG) in zwei Verfahren mit dem „Recht auf Vergessen" beschäftigt; beide **Beschlüsse vom 6.11.2019** haben weitreichende Bedeutung.

63 Im ersten Fall (**1 BvR 16/13; Recht auf Vergessen I**[33]) ergibt sie sich in erster Linie aus den Feststellungen des BVerfG zur Reichweite seiner Prüfungskompetenz in Bezug auf die Auslegung europäischen Rechts und insoweit sein Verhältnis zum EuGH. In materiellrechtlicher Hinsicht verortet das BVerfG den verfassungsrechtlichen Maßstab für den Schutz gegenüber Gefährdungen durch die Verbreitung personenbezogener Berichte und Informationen als Teil öffentlicher Kommunikation in den äußerungsrechtlichen Ausprägungen des allgemeinen Persönlichkeitsrechts, nicht im Recht auf informationelle Selbstbestimmung und damit im Datenschutzrecht (Urt. Rn. 92). Die Verbreitung von Berichten über Vorgänge des öffentlichen Lebens unterfalle der Meinungsfreiheit nach Art. 5 Abs. 1 Satz 1 GG. Zugleich sei die Pressefreiheit nach Art. 5 Abs. 1 Satz 2 GG berührt, die die Presse über die Meinungsäußerungsfreiheit hinaus in ihrer institutionellen Eigenständigkeit schütze. Dazu gehöre auch die Entscheidung eines Presseverlags, frühere Presseberichte der Öffentlichkeit dauerhaft in Archiven zugänglich zu machen. Über die Publikation allein des Inhalts der Berichte hinaus liege hierin eine gewichtige selbstständige Entscheidung eines Verlagshauses über die Form der Verbreitung seiner Produkte und damit sowohl über deren Wirkung als auch über seine eigene Wahrnehmbarkeit (Urt. Rn. 94). Demgegenüber sei die Freiheit der Rundfunkberichterstattung nach Art. 5 Abs. 1 Satz 2 GG im betreffenden Fall nicht berührt. Denn ihr sei die Verbreitung von Informationen nicht schon immer dann zuzuordnen, wenn sie sich dafür elektronischer Informations- und Kommunikationssysteme bediene. Die Einstellung eigener Berichte in ein Onlinearchiv oder deren Zugänglichmachung über das Internet (bspw. über YouTube) mache sie nicht deswegen schon zu „Rundfunk" im Sinne der Verfassung (Urt. Rn. 95).

64 Dabei habe unter den Kommunikationsbedingungen des Internet die seit der ursprünglichen Veröffentlichung vergangene Zeit ein spezifisches Gewicht. Denn anders als früher blieben einmal online veröffentlichte Informationen heute dauer-

[33] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/11/rs20191106_1bvr001613.html

haft verfügbar, jederzeit abrufbar und beliebig verknüpfbar. Die damit verbundenen Folgen für die öffentliche Kommunikation reichten weit und änderten die Bedingungen der freien Entfaltung der Persönlichkeit tiefgreifend. Die Rechtsordnung müsse eine Person davor schützen, dass die Öffentlichkeit ihr frühere Positionen, Äußerungen oder Handlungen unbegrenzt lang vorhalten könne. Insbesondere könne eine Bereitschaft zur Mitwirkung in Staat und Gesellschaft nur erwartet werden, wenn in dieser Hinsicht ein hinreichender Schutz gewährleistet sei. Was für das Recht auf informationelle Selbstbestimmung gelte, gelte insoweit für das allgemeine Persönlichkeitsrecht allgemein (Urt. Rn. 101 ff.). Daraus folge allerdings kein allgemeiner Anspruch darauf, die Veröffentlichung personenbezogener Daten nur nach Maßgabe eigener Maßstäbe zuzulassen. Generell komme es auf eine Abwägung aller Interessen zum Zeitpunkt der jeweiligen Veröffentlichung an, bei der auch die Bedeutung von Onlinearchiven für die öffentliche Meinungsbildung zu berücksichtigen sei (Urt. Rn. 107 ff.).

65 In praktischer Hinsicht bedeutsam sind die Feststellungen des BVerfG zu den Sorgfaltspflichten der Anbieter von Onlinearchiven. Denn es befreit insbesondere Verlage – und entsprechendes gilt dann auch für die Rundfunkanstalten – ausdrücklich davon, ein solches Archiv ihrerseits laufend daraufhin zu überprüfen, ob ein anfänglich rechtmäßig veröffentlichter Bericht zwischenzeitlich unzulässig geworden sein könnte. Vielmehr hält das BVerfG eine dahingehende Prüfung nur auf eine „qualifizierte Beanstandung" der betroffenen Person hin für erforderlich, aus der ihre Schutzbedürftigkeit und damit auch zugleich der Kontrollrahmen hervorgehe (Urt. Rn. 109).

66 Die in einem solchen Fall ausgelösten Handlungspflichten des Verlags (bzw. der Rundfunkanstalt) ordnet das BVerfG in das Spannungsfeld zwischen dem Interesse der Presse (bzw. Rundfunks) und der Allgemeinheit an einer vollständigen und unveränderten Dokumentation des öffentlichen Geschehens einerseits sowie andererseits dem Interesse der betroffenen Person ein, nicht dauerhaft uneingeschränkt mit Vorgängen aus der Vergangenheit konfrontiert zu werden. Insbesondere sei zu prüfen, ob der Anbieter eines Onlinearchivs in einem solchen Fall durch zumutbare Vorkehrungen dafür sorgen könne, die zumindest gegen die Auffindbarkeit der betreffenden Berichte durch Suchmaschinen bei namensbezogenen Suchabfragen einen gewissen Schutz bieten, ohne die Auffindbarkeit und Zugänglichkeit des Berichts im übrigen übermäßig zu hindern (Urt. Rn. 129 ff.).

67 Im zweiten Verfahren (**1 BvR 276/17; Recht auf Vergessen II**[34]) ging es um die Frage, ob und inwieweit ein Suchmaschinenanbieter – hier: Google – verpflichtet

[34] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/11/rs20191106_1bvr027617.html;jsessionid=070D90A81B2540171BA38262E1ECCFE8.2_cid361

werden kann, die Anzeige eines Suchergebnisses mit personenbezogenen Daten, insbesondere einer Namensnennung, zu unterlassen. Auslöser war in diesem Fall das online unverändert abrufbare Manuskript eines Beitrags des ARD-Magazins „Panorama" aus dem Jahr 2010, in dem unter anderem auf der Basis eines mit ihr geführten Interviews Vorwürfe gegen eine namentlich genannte Person erhoben wurden. Das BVerfG bekräftigt zunächst die Rechtsprechung des EuGH (C 131/12 – Google Spain), nach der Datenverarbeitung durch Suchmaschinenanbieter nicht journalistischen Zwecken diene (Urt. Rn. 36); auch auf die Meinungsfreiheit können sie sich nicht berufen, da der Zweck der Suchmaschinen nicht darin bestehe, Meinungen zu verbreiten (Urt. Rn. 105). Ebenso wenig wie die Anbieter von Onlinearchiven hält das BVerfG Suchmaschinenbetreiber für verpflichtet, sich von sich aus laufend davon zu überzeugen, dass die von ihnen generierten Suchergebnisse auf zulässige Veröffentlichungen hinweisen; vielmehr müsse ein dahingehender Anspruch gegen sie geltend gemacht werden (Urt. Rn. 113). In einem solchen Fall seien in die gebotene Abwägung neben den Persönlichkeitsrechten der betroffenen Person (Art. 7 und 8 GRCh) im Rahmen der unternehmerischen Freiheit der Suchmaschinenbetreiber (Art. 16 GRCh) die Grundrechte der jeweiligen Inhalteanbieter sowie die Informationsinteressen der Internetnutzer einzubeziehen (Urt. Rn. 115 ff.).

68 Das **Bundesverwaltungsgericht** (BVerwG) hatte in einem schon seit 2011 anhängigen Verwaltungsrechtsstreit im Jahr 2018 mittels eines Vorabentscheidungsverfahrens den EuGH zur Klarstellung veranlasst, dass der Betreiber einer Facebook-Fanpage datenschutzrechtlich als „Verantwortlicher" zu qualifizieren ist (EuGH, Urteil vom 5.6.2018, C-210/16[35]). Danach erfasst dieser Begriff auch Stellen, die anderen Gelegenheit zur Datenverarbeitung geben, ohne selbst damit befasst zu sein. Der Umstand, dass ein Fanpagebetreiber lediglich die von Facebook eingerichtete Plattform nutzt, befreit ihn nicht davon, seine datenschutzrechtlichen Verpflichtungen zu beachten (EuGH Rn. 40). Im Ergebnis sind demzufolge Facebook und die Fanpagebetreiber jeweils gemeinsam verantwortlich.

69 Auf dieser Grundlage befasste sich das BVerwG anschließend erneut und abschließend mit den daraus folgenden aufsichtsrechtlichen Konsequenzen. In seinem **Urteil vom 11.9.2019**[36] stellte es fest, dass eine nationale Kontrollbehörde dann, wenn ihr – wie hier – infolge einer gemeinsamen Verantwortlichkeit mehrere potentielle Adressaten für eine Abhilfemaßnahme zur Verfügung stehen, unter Beachtung des Verhältnismäßigkeitsprinzips nach pflichtgemäßem Ermessen über die Auswahl entscheiden müsse (Urt. Rn. 20 ff.). Dabei könne sie sich legitimerweise auf den das Gefahrenabwehrrecht beherrschenden Gedanken der Effektivität stüt-

[35] http://curia.europa.eu/juris/document/document.jsf;jsessionid=6DFC4C8ED2D42BA60A4946F9A08C9517?text=&docid=202543&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=4457334

[36] https://www.bverwg.de/de/110919U6C15.18.0

zen und sich von der Erwägung leiten lassen, dass ein rechtswidriger Zustand durch die Inanspruchnahme eines bestimmten Adressaten schneller oder wirksamer beseitigt werden könne. Datenschutzrechtliche Verstöße Dritter ließen die Verantwortlichkeit für das jeweils eigene Angebot unberührt; einen Anspruch auf Gleichbehandlung im Unrecht gebe es nicht. Daher sei die Aufsichtsbehörde auch nicht gehalten, vor einer Inanspruchnahme des einen Verantwortlichen (hier: des Fanpagebetreibers) ein Konzept für ein flächendeckendes Vorgehen gegen alle anderen Fanpagebetreiber in seiner Zuständigkeit zu entwickeln (Urt. Rn. 30 ff.)

70 Mit „Facebook und den (rechtlichen) Folgen" befasste sich auch das **Bundeskartellamt** (BKartA). Sein **Beschluss vom 6.2.2019** (Bs-22/16[37]) erregte über Deutschland hinaus Aufsehen, weil damit erstmals die Umstände einer Verarbeitung personenbezogener Daten Gegenstand einer kartellrechtlichen Untersagungsverfügung wurden. Denn das BKartA untersagte Facebook dort die Verwendung der Nutzungsbedingungen, auf deren Grundlage das Unternehmen personenbezogene Daten seiner Nutzer erfasste und über alle Facebook-Produkte hinweg miteinander verknüpfte und verwendete. Angesichts der marktbeherrschenden Stellung von Facebook sei der Einsatz der Nutzungsbedingungen missbräuchlich; die insoweit relevante Vorschrift des § 19 Abs. 1 GWB sei neben den Regelungen der DSGVO anwendbar. Die formal erteilte Einwilligung der Nutzer mit den von Facebook vorgegebenen Bedingungen könne angesichts der Marktmacht von Facebook nicht als freiwillig im Sinne von Art. 6 Abs. 1 S. 1 lit. a) DSGVO qualifiziert werden.

71 Allerdings wurde dieser Beschluss bislang nicht wirksam, denn im anschließenden vorläufigen Rechtsschutzverfahren setzte ihn das **OLG Düsseldorf** mit **Beschluss vom 26.8.2019** - VI Kart 1/19 (V)[38] – wegen durchgreifender Zweifel an seiner Rechtmäßigkeit aus. Zwar sei es nicht von vorherein ausgeschlossen, eine Schädigung des Verbraucherschutzes als einen relevanten Wettbewerbsschaden im Sinne von § 19 Abs. 1 GWB aufzufassen. Einen solchen rufe das Verhalten von Facebook hier jedoch nicht hervor, denn die personenbezogenen Daten der Nutzer seien jederzeit duplizierbar und deshalb nicht einem Entgelt gleichzustellen. Zudem erteilten die Nutzer Facebook ihre Zustimmung nicht wegen dessen Marktmacht, sondern als Resultat einer individuellen Abwägung der damit verbundenen Vor- und Nachteile. Daher sei davon auszugehen, dass der Bescheid im Hauptsachverfahren aufgehoben werden müsse.

[37] https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf;jsessionid=46B51065D3D64EF6A2F5CF4D1AE455D2.1_cid378?__blob=publicationFile&v=8

[38] https://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf

72 Unbeschadet dieser recht ernüchternden ersten gerichtlichen Bewertung des Sachverhalts hoffe ich sehr, dass die Diskussion um das Verhältnis von Kartell- bzw. Wettbewerbs- zum Datenschutzrecht damit erst eingeleitet und nicht etwa bereits wieder beendet worden ist. Denn unter anderem die im Hintergrund stehende Frage nach der (wirtschaftlichen) Bewertung und (wettbewerbsrechtlichen) Einordnung personenbezogener Daten hat grundsätzliche Bedeutung, ebenso wie die Frage, wie es um die „Freiwilligkeit" einer Einwilligung in monopolistischen Kommunikationsstrukturen bestellt ist. Im Interesse der Verbraucher und Nutzer ist zu hoffen, dass künftig datenschutzrechtliche Vorgaben als wettbewerbsrelevant qualifiziert und deshalb auch mithilfe kartellrechtlicher Instrumente durchgesetzt werden können.

73 Schließlich sei hier noch auf zwei im Jahr 2019 veröffentlichte **Gutachten** mit Bezügen zum Datenschutz hingewiesen:

74 Zum einen ist insoweit ein im Auftrag des BMJV entstandenes Gutachten vom 30. September 2019 zur **Untersuchung der Umsetzung der DSGVO durch Online-Dienste** zu nennen[39]. Die Autoren der Universität Göttingen überprüften im Zeitraum Juni bis September 2019 insgesamt 35 relevante Online-Angebote daraufhin, ob und inwieweit dort die Vorgaben der DSGVO berücksichtigt wurden. Zu den fünf überprüften „Informationsportalen" gehörte außer Bild.de, Spiegel online, Focus Online und WetterOnline auch ard.de bzw. Das Erste.de (S. 75, 183 ff.). Alle Angebote wurden auf fünf Themen hin untersucht: Informationspflichten und Datenschutzerklärung, Angabe der Datenverarbeitung und der jeweiligen Rechtsgrundlagen, Einwilligung der Betroffenen, Umgang mit sensiblen Daten und datenschutzfreundliche Voreinstellungen. Die Ergebnisse ordnete die Studie jeweils auf einer Skala zwischen 1 (nicht erfüllt) und 5 (mehr als erfüllt) ein. Keiner der untersuchten Dienste erfüllte alle einschlägigen Anforderungen der DSGVO, in zahlreichen Punkten zeigte sich noch erheblicher Optimierungsbedarf. Das galt auch für den Auftritt von „daserste.de", dem das Gutachten (wie auch bild.de und Spiegel-Online) lediglich eine Gesamtbewertung mit 2-3 attestiert.

75 Zum anderen veröffentlichte im November 2019 die am 18. Juli 2018 von der Bundesregierung eingesetzte **Datenethikkommission** (DEK) ihr Gutachten für einen Entwicklungsrahmen zur Datenpolitik sowie den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen[40]. Von den zahlreichen Empfehlungen seien hier nur einige hervorgehoben:

[39] https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/112919_DSGVO_Studie.pdf?__blob=publicationFile&v=2

[40] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=17D0F7FCA5977A07E73CA2A39650583E.1_cid295?__blob=publicationFile&v=6

76 * Die DEK empfiehlt Maßnahmen gegen ethisch nichtvertretbare Datennutzungen. Dazu gehören etwa Totalüberwachung, die Integrität der Persönlichkeit verletzende Profilbildung, gezielte Ausnutzung von Vulnerabilitäten, sog. Addictive Designs und Dark Patterns, dem Demokratieprinzip zuwiderlaufende Beeinflussung politischer Wahlen, Lock-in und systematische Schädigung von Verbrauchern sowie viele Formen des Handels mit personenbezogenen Daten.

77 * Die DEK weist darauf hin, dass sowohl das Datenschutzrecht als auch die übrige Rechtsordnung (u. a. Zivilrecht, Lauterkeitsrecht) bereits eine Fülle von Instrumenten vorsieht, die gegen derartige Datennutzungen eingesetzt werden können. Gemessen an Breitenwirkung und Schädigungspotenzial würden diese Instrumente indessen bislang nicht ausreichend genutzt – insbesondere gegenüber marktmächtigen Unternehmen (s. dazu oben Rn. 45). Dieses Vollzugsdefizit habe verschiedene Ursachen, die es systematisch anzugehen gelte.

78 * Neben der Schärfung des Bewusstseins bei handelnden Akteuren (z. B. Aufsichtsbehörden) für die bereits bestehenden Möglichkeiten sei dringend eine Konkretisierung und punktuelle Verschärfung des geltenden Rechtsrahmens angezeigt. Dazu gehörten etwa eine spezielle Normierung datenspezifischer Klauselverbote, Schutz- und Treuepflichten, Deliktstatbeständen und unlauteren Geschäftspraktiken sowie die Schaffung eines weitaus konkreteren Rechtsrahmens für Profilbildungen und Scoring wie auch für den Datenhandel.

79 * Um die Wirkungskraft der Aufsichtsbehörden zu erhöhen, müssten diese weitaus besser personell und sachlich ausgestattet werden. Sofern es nicht gelinge, die Abstimmung unter den deutschen Datenschutzaufsichtsbehörden zu verstärken und zu formalisieren und so die einheitliche und kohärente Anwendung des Datenschutzrechts zu gewährleisten, sei eine Zentralisierung der Datenschutzaufsicht für den Markt in einer – mit einem weiten Mandat ausgestatteten und eng mit anderen Fachaufsichtsbehörden kooperierenden – Behörde auf Bundesebene zu erwägen. Die Zuständigkeit der Landesdatenschutzbehörden für den öffentlichen Bereich solle hingegen unangetastet bleiben.

dd) Datenschutzprobleme

80 Einer im Auftrag des Branchenverbands Bitkom entstandenen repräsentativen Umfrage zufolge ist im Jahr 2018 jeder zweite Internetnutzer Opfer von Cyberkriminalität geworden[41]. Zahlreiche aufsehenerregende Datenschutzvorfälle führten der Öffentlichkeit – und den Betroffenen selbst – auch im vergangenen Jahr vor Augen, wie enorm das Gefährdungspotential für personenbezogene Daten in einer digitalisierten und zunehmend vernetzten Welt mittlerweile ist.

---

[41] https://bitkom.de/Presse/Presseinformation/Mehr-zweite-Onliner-Opfer-Cyberkriminalitaet

81 Schon kurz nach Jahresbeginn wurde bekannt, dass rund 1000 Prominente Opfer eines Hackerangriffs geworden waren[42], und wenig später waren die Passwörter und mail-Adressen von etwa 773 Millionen Onlinenutzern für etwa 12.000 Onlinedienste im Internet frei zugänglich[43]. Im September und Dezember konnte jeder Interessierte jeweils über längerer Zeit die Daten von hunderten von Millionen unterschiedlicher Facebook-Nutzer im Netz einsehen [44]. Facebook war auch involviert, als der Blutspendedienst des Bayerischen Roten Kreuzes, offenbar infolge einer versehentlich falschen Programmierung seiner Onlineseite, im Sommer gesundheitsbezogene Daten möglicher Spender – etwa zu HIV-Infektionen, Schwangerschaften, Drogenkonsum oder Diabetes - an Facebook weiterleitete[45] .

82 Besonders beunruhigend aber ist die Erkenntnis, wie stark heutzutage auch die besonders sensible und für die Funktionsfähigkeit des Rechtsstaats unentbehrliche Datenverarbeitung in öffentlichen Einrichtungen wie Behörden oder Gerichten gefährdet ist. Dies zeigten zahlreiche Cyberattacken mit der berüchtigten Schadsoftware „Emotet“. Wiederholt und eindringlich warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI)[46] vor diesem besonders gefährlichen Datenvirus, mithilfe dessen die Zugangsdaten für infizierte mail-Konten sowie deren Inhalte ausgespäht und von dort vermeintlich authentische Antworten auf offizielle mails versandt werden, die die Schadsoftware weiter verbreiten. Den eigentlichen Schaden richten die Täter dann mit nachgeladener Software an, meist zunächst einem Trojaner, der ihnen den Zugriff auf das gesamte Betriebsnetzwerk verschafft, bevor sie manuell den Zugang blockieren oder sogenannte Ransomware einsetzen. Dabei verschlüsselt der Trojaner sämtliche Daten, legt ganze Netzwerke lahm und fordert Lösegeld. Betroffen von einer derartigen Attacke waren nicht nur unzählige Privatpersonen, kleine und große Betriebe - darunter einige Einrichtungen in meinem Zuständigkeitsbereich (dazu unten Rn. 217) -, sondern auch die Verwaltung der Stadt Potsdam oder – besonders gravierend – das Kammergericht in Berlin.

83 In diesem Zusammenhang sei noch erwähnt, dass die staatlichen Datenschutzaufsichtsbehörden inzwischen in den ihnen bekannt gewordenen Fällen von Datenschutzverstößen sukzessive die von Art. 58 Abs. 2 DSGVO zur Verfügung gestellten Abhilfebefugnisse und hier insbesondere den durch Art. 58 Abs. 2 lit. i) in Verbindung mit Art. 83 DSGVO eröffneten Bußgeldrahmen konkretisieren bzw. ausschöpfen, der weit über den vormaligen des BDSG hinausgeht. Die DSK hat dazu

42 https://www.sueddeutsche.de/digital/datenklau-hackerangriff-orbit-doxing-1.4277639
43 https://www.tagesschau.de/ausland/internet-sicherheit-cybercrime-101.html
44 https://www.heise.de/newsticker/meldung/Daten-von-267-Millionen-Facebook-Nutzern-offen-im-Netz-4621213.html
45 https://www.sueddeutsche.de/digital/blutspende-brk-facebook-patientendaten-1.4576563
46 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Emotet-Warnung_230919.html
https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html

ein Konzept zur Bemessung von Bußgeldern[47] veröffentlicht, an dem sich die Praxis der staatlichen Aufsichtsbehörden orientieren soll. In zahlreichen Fällen haben sie inzwischen bereits Bußgelder in teilweise erheblicher Höhe verhängt. Ein vergleichbarer Katalog der Rundfunkdatenschutzbeauftragten soll noch entstehen.

2 Datenschutz und Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk

a Bedeutung des Datenschutzes für den öffentlich-rechtlichen Rundfunk

84 Seine spezifische verfassungsrechtliche Legitimation berechtigt den öffentlich-rechtlichen Rundfunk ebenso wie sie ihn verpflichtet. In datenschutzrechtlicher Hinsicht sehe ich das beispielsweise in Bezug auf die folgenden Themen als relevant an:

85 Die Allgemeinheit finanziert den öffentlich-rechtlichen Rundfunk mit dem Rundfunkbeitrag, der grundsätzlich für jede Wohnung oder Betriebsstätte fällig ist. Der dazu eingerichtete Beitragsservice von ARD, ZDF und Deutschlandradio verwaltet über 40 Millionen Beitragskonten. Die Bevölkerung muss sich darauf verlassen können, dass die Rundfunkanstalten diesen enormen Datenbestand ausschließlich für den Einzug des Rundfunkbeitrags verarbeiten und vor dem Zugriff Dritter schützen.

86 Der Rundfunkbeitrag dient der Finanzierung einer umfassenden, zuverlässigen und objektiven Berichterstattung für die gesamte Bevölkerung durch den öffentlich-rechtlichen Rundfunk. Glaubwürdigkeit und Integrität seiner Angebote gehören zum Kern seines verfassungsrechtlichen Funktionsauftrags. Die Allgemeinheit muss sich darauf verlassen können, dass die Rundfunkanstalten auf verifizierte Quellen und gesicherte Datenbestände zurückgreifen und personenbezogene Daten nur im zulässigen Umfang zugänglich machen.

87 Sein Funktionsauftrag berechtigt und verpflichtet den öffentlich-rechtlichen Rundfunk dazu, die Bevölkerung auf allen für den publizistischen Wettbewerb der elektronischen Medien relevanten Wegen mit seinem Angebot versorgen. Dazu gehören seit geraumer Zeit selbstverständlich auch die vielfältigen Verbreitungs- und Darstellungsoptionen über das Internet. Die Onlinenutzer müssen sich darauf verlassen können, dass die Rundfunkanstalten ihre personenbezogenen Daten dort nur im zulässigen Umfang verarbeiten und dies auch Dritten, auf deren Dienste sie zurückgreifen, nur in diesem Umfang gestatten. Sie dürfen außerdem erwarten,

[47] https://www.datenschutzkonferenz-online.de/media/ah/20191016_bußgeldkonzept.pdf

dass die Rundfunkanstalten überall dort, wo sie sie zur Nutzung von Plattformen Dritter veranlassen, über damit verbundene Datenschutzrisiken aufklären.

88 Wie jede öffentlich-rechtliche Einrichtung unterliegen die Rundfunkanstalten spezifischen gesetzlichen Verpflichtungen im Verhältnis zu ihren (fest oder frei) Beschäftigten und Auftragnehmern. Diese müssen sich jeweils darauf verlassen können, dass die Rundfunkanstalten besonders gewissenhaft mit den ihnen anvertrauten personenbezogenen Daten umgehen und sie ausschließlich im Rahmen des jeweiligen Vertragsverhältnisses verarbeiten.

89 Zusammenfassend gesagt: Institutionell ist der öffentlich-rechtliche Rundfunk in Deutschland im Sinne der Rechtsprechung des BVerfG „staatstragend". Ob er diese Rolle glaubwürdig erfüllen kann, hängt nicht zuletzt davon ab, inwieweit er in der Lage ist, Datenschutz zuverlässig zu gewährleisten. Insofern ist ein wirksamer umfassender Datenschutz für den öffentlich-rechtlichen Rundfunk systemrelevant.

90 Das gilt grundsätzlich auch für den Beteiligungsbereich der Rundfunkanstalten. Seine Beteiligungsunternehmen haben eine unterstützende Funktion im weiteren Bereich des öffentlich-rechtlichen Funktionsauftrags. Sie sind zudem – ungeachtet der gebotenen strikten finanziellen Trennung – funktional eng mit den Rundfunkanstalten verflochten und insoweit Teil des „Systems öffentlich-rechtlicher Rundfunk", besonders natürlich, aber keineswegs nur im Bereich der Programmproduktion.

b Spezifische Datenschutzaufsicht sichert die Unabhängigkeit

91 Der öffentlich-rechtliche Rundfunk in Deutschland muss gemäß Artikel 5 Abs. 1 S. 2 GG und der Rechtsprechung des Bundesverfassungsgerichts staatsfern organisiert sein. Im Sinne einer optimalen Umsetzung dieses Gebots unterliegen die meisten Rundfunkanstalten auch nicht der Aufsicht der staatlichen Datenschutzbehörden. Ausnahmeregelungen gibt es nur bei den Landesrundfunkanstalten Hessischer Rundfunk, Radio Bremen und Rundfunk Berlin-Brandenburg sowie dem Auslandssender des Bundes, der Deutschen Welle; dort ist lediglich die Datenverarbeitung zu journalistischen Zwecken von der Aufsicht durch die jeweilige staatliche Datenschutzbehörde ausgenommen. Diese Konstruktion ist nicht nur, wie bereits ausgeführt (oben Rn. 30) mit Blick auf das Gebot der Staatsferne unbefriedigend, sondern auch deshalb, weil sie die ohnehin föderal ausdifferenzierte Aufsichtsstruktur in Bezug auf die Rundfunkanstalten unnötigerweise noch heterogener macht. Außerdem erzeugen diese Sonderregelungen Abgrenzungsschwierigkeiten zur Zuständigkeit in Bezug auf den absolut geschützten Bereich der journalistischen Datenverarbeitung in materiell rechtlicher sowie zusätzlichen Abstimmungs- und Klärungsaufwand in formell rechtlicher Hinsicht (zB. Zuständigkeit für Meldun-

gen nach Art. 33 DSGVO sowie im Beteiligungsbereich).

92 Maßgebend für die Ausgestaltung der Datenschutzkontrolle im öffentlich-rechtlichen Rundfunk sind die Vorgaben der DSGVO sowie die für die jeweilige Rundfunkanstalt geltenden gesetzlichen Vorschriften. Der DSGVO liegt dabei ein Leitbild zugrunde, das von einer unabhängigen Kontrolle und der Bewertung bzw. Entscheidung grundsätzlicher Fragen durch eine strukturell unabhängige Aufsicht einerseits sowie die interne Überwachung und Beratung, Unterstützung und Einzelfallbewertung des „operativen Datenschutzes" durch funktional unabhängige interne Datenschutzbeauftragte andererseits ausgeht. Die Aufgaben der Aufsicht und die der internen Datenschutzbeauftragten greifen insoweit also ineinander, sind aber zugleich in ihrer jeweiligen Selbstständigkeit und Unabhängigkeit auch stärker profiliert als zuvor (s. bereits oben Rn. 19).

93 Dementsprechend hat sich auch die Aufsichtsstruktur im öffentlich-rechtlichen Rundfunk verändert: seit dem Inkrafttreten der DSGVO ist bei den meisten Rundfunkanstalten schon gesetzlich die Aufsicht von einem Rundfunkdatenschutzbeauftragten, der operative Datenschutz von einem internen Datenschutzbeauftragten wahrzunehmen. Die Rechtsstellung des jeweiligen Rundfunkdatenschutzbeauftragten entspricht der der staatlichen Datenschutzbeauftragten. Während diese vom Bundestag bzw. jeweiligen Landtag gewählt werden, ist dafür bei den in der ARD zusammengeschlossenen Rundfunkanstalten der Rundfunkrat, beim ZDF der Fernsehrat sowie beim Deutschlandradio der Hörfunkrat zuständig. Zusätzlich muss der Bestellung in einigen Rundfunkanstalten auch noch der Verwaltungsrat zustimmen.

94 Die gegen diese Konstruktion vereinzelt[48] bemühten Bedenken bezüglich der Unabhängigkeit der Aufsicht im öffentlich-rechtlichen Rundfunk entbehren jeder Grundlage. Anders als früher liegt die Umsetzung der gesetzlichen Vorgaben zur Aufsicht jetzt ausschließlich bei den Gremien der (von ihnen zu beaufsichtigenden) Rundfunkanstalten; diese selbst sind an dem Verfahren und der Ausgestaltung nicht mehr beteiligt. Alle maßgeblichen Vorkehrungen, die die Unabhängigkeit der Rundfunkdatenschutzbeauftragten sichern, entsprechen denen der staatlichen Aufsichtsbehörden. Gleiches gilt für ihre Aufgaben und Befugnisse.

c Datenschutzbeauftragte nach Art. 37 DSGVO

95 Wie bereits erwähnt, sieht das jeweils maßgebliche Landesrecht für alle Rundfunkanstalten in meinem Zuständigkeitsbereich die Bestellung eines internen Daten-

[48] Siehe Abschnitt 1.3, S. 22 f. des 24. Datenschutz- und Informationsfreiheitsberichts der Beauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen für die Jahre 2017/2018, https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/24_DIB-2019/24_-DIB-2019-1.pdf

schutzbeauftragten vor; es kann deshalb dahinstehen, ob dies nicht bereits unmittelbar nach Art. 37 Abs. 1 lit. a) DSGVO geboten wäre, nach der „Behörden oder öffentliche Stellen" diese Funktion zwingend einzurichten haben. Die Artt. 38 und 39 DSGVO haben die Stellung und Aufgaben des Datenschutzbeauftragten gegenüber dem status quo ante noch einmal deutlich geschärft und seine Unabhängigkeit bekräftigt (siehe dazu auch unten Rn. 211 ff.). Er kontrolliert die Einhaltung der Datenschutzvorschriften bei der gesamten Tätigkeit der Rundfunkanstalt und berät und unterstützt alle Fachbereiche dabei. Er ist in der Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen.

96 Außerdem haben die Verantwortlichen für einige rechtlich unselbstständige Gemeinschaftseinrichtungen der öffentlich-rechtlichen Rundfunkanstalten eigene Datenschutzbeauftragte bestellt bzw. die Zuständigkeit ihrer internen Datenschutzbeauftragten auf solche Gemeinschaftseinrichtungen erweitert. Für den Beitragsservice von ARD, ZDF und Deutschlandradio schreibt § 11 Abs. 2 Rundfunkbeitragsstaatsvertrag (RBStV) eine solche Funktion ausdrücklich vor. Dies ist sachgerecht, weil ein umfassender Datenschutz im Zusammenhang mit dem Einzug des Rundfunkbeitrags für die Akzeptanz des öffentlich-rechtlichen Rundfunks essentiell und deshalb eine funktionale Absicherung durch die Bestellung eines eigenen internen Datenschutzbeauftragten sinnvoll ist.

97 Der Beitragsservice verwaltet sämtliche für den Beitragseinzug erforderlichen Daten aller Beitragspflichtigen in Deutschland und damit einen außerordentlich großen Datenbestand. Die dafür maßgeblichen datenschutzrechtlichen Vorgaben enthält der RBStV. Anders als vielfach wahrgenommen, ist der Beitragsservice keine juristische Person, sondern eine nichtrechtsfähige Verwaltungseinrichtung. Sie wird im Außenverhältnis im Rahmen des Beitragsfestsetzungs- und gegebenenfalls -vollstreckungsverfahrens quasi als verlängerter Arm der jeweils zuständigen Landesrundfunkanstalt in deren Auftrag und damit hoheitlich tätig.

98 Die durch die Ende 2019 in Kraft getretene Neufassung von § 38 BDSG angehobene Relevanzschwelle für die obligatorische Bestellung einer oder eines Datenschutzbeauftragten (s.o. Rn. 33) ist auch für die Beteiligungsgesellschaften der Rundfunkanstalten maßgeblich. Angesichts ihrer Zugehörigkeit zum „System öffentlich-rechtlicher Rundfunk" (oben Rn. 90) sollten die Verantwortlichen aber im Zweifel von der durch die DSGVO eröffneten Möglichkeit Gebrauch machen, die Funktion freiwillig zu besetzen. Denn dies sichert nicht nur sie selbst in ihrem unmittelbaren Verantwortungsbereich ab, sondern kommt auch der Verlässlichkeit des „Systems" insgesamt zugute.

99 Dies gilt ganz entsprechend auch für die Gemeinschaftseinrichtungen der Rundfunkanstalten. Sie sind zwar rechtlich unselbstständig und deshalb für sich genommen nicht Adressat der gesetzlichen Vorgaben; datenschutzrechtlich verant-

wortlich sind in vollem Umfang die Intendantinnen und Intendanten der jeweils beteiligten Rundfunkanstalten. Allerdings treten einige dieser Gemeinschaftseinrichtungen zumindest im Außenverhältnis wie eigenständige Organisationen auf und sind teilweise auch organisatorisch recht weitgehend verselbstständigt. Sowohl in der Außenwahrnehmung wie auch im Binnenverhältnis zu den für sie verantwortlichen Rundfunkanstalten ähnelt ihr Status in datenschutzrechtlicher Hinsicht daher eher dem eines Beteiligungsunternehmens als dem einer Organisationseinheit der betreffenden Rundfunkanstalten.

100 Die Anforderungen an die mit der Funktion des internen Datenschutzbeauftragten betraute Person definiert Art. 37 Abs. 5 DSGVO. Anders als die Aufsicht kann sie nach Art. 38 Abs. 6 DSGVO auch anderweitige Aufgaben in der Organisation übernehmen. Von dieser Option haben die Rundfunkanstalten überwiegend, die Beteiligungsgesellschaften durchgängig Gebrauch gemacht. Die Vorgaben zur organisatorischen Einbindung des Datenschutzbeauftragten enthält Art. 38 DSGVO.[49]

101 Die Kriterien, nach denen die Verantwortlichen über die freiwillige Bestellung eines Datenschutzbeauftragten entscheiden sollten, sind in einer von mir entworfenen Handreichung der RDSK zusammengetragen[50]. Zu berücksichtigen ist dabei, dass der Status freiwillig bestellter Datenschutzbeauftragter vollständig dem der gesetzlich zwingend zu benennenden entspricht.

d Exkurs: Datenschutzaufsicht bei den sonstigen Medien

102 Noch unterschiedlicher als im öffentlich-rechtlichen Rundfunk haben die Länder die Datenschutzaufsicht über private Veranstalter von Rundfunk und Telemedien ausgestaltet. Die Bandbreite reicht hier von einer bei der jeweiligen Landesmedienanstalt angesiedelten autonomen Datenschutzaufsicht durch einen Mediendatenbeauftragten als Pendant zum jeweiligen Rundfunkdatenschutzbeauftragten (in diesem Falle: jeweils zu mir, da dieses Modell nur in Bayern, Nordrhein-Westfalen und im Saarland umgesetzt wurde) über die Wahrnehmung dieser Aufgabe durch die Landesmedienanstalt selbst bis hin zur Aufsicht durch den Landesdatenschutzbeauftragten.

103 Presseverlage wiederum unterliegen nach den Vorgaben des jeweiligen Landespressegesetzes seit jeher keiner „originären" Datenschutzkontrolle, wenn und so-

[49] Siehe im übrigen zu den bei der Bestellung interner Datenschutzbeauftragter zu berücksichtigenden Aspekten das Kurzpapier Nr. 12 der DSK vom Dezember 2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf

[50] https://www.rundfunkdatenschutz.de/infothek/kriterien-bestellung-dsb.file.html/Kriterien%20Bestellung%20DSB%2020191218.pdf

weit sie sich der freiwilligen Selbstkontrolle durch den Deutschen Presserat unterworfen haben. Dies gilt auch hinsichtlich der von ihnen verantworteten Telemedienangebote. Auf der Basis von Art. 85 DSGVO haben die Länder diese Sonderkonstruktion auch nach Inkrafttreten der DSGVO weiterbestehen lassen, obwohl sie einer unabhängigen Datenschutzaufsicht im Sinne von Art. 51 DSGVO funktional nicht vergleichbar ist. Der Presserat hat einen Pressekodex, einen Leitfaden zum Redaktionsdatenschutz und eine Beschwerdeordnung erlassen, auf deren Grundlage er an ihn gerichtete Datenschutzbeschwerden prüft und bescheidet.

3 Der Gemeinsame Rundfunkdatenschutzbeauftragte

104 Seit Januar 2019 nehme ich gemeinsam für BR, SR, WDR, Deutschlandradio und ZDF sowie die von ihnen verantworteten Gemeinschaftseinrichtungen und ihre Beteiligungsunternehmen das Amt des Rundfunkdatenschutzbeauftragten wahr. Zuständig für die Wahl sind die Gremien der Rundfunkanstalten. Ihre Zuständigkeit entspricht im System öffentlich-rechtlicher Rundfunk insoweit der Rolle der Landtage im staatlichen Bereich und verhindert, dass – anders als vor Inkrafttreten der DSGVO - der datenschutzrechtlich Verantwortliche (Intendant) bei der Besetzung der Aufsichtsposition mitwirkt.

105 Für den Bayerischen Rundfunk hat mich der Rundfunkrat mit Zustimmung des Verwaltungsrats (Art. 21 BR-Gesetz), für den Saarländischen Rundfunk (§ 42b SMG) und den Westdeutschen Rundfunk der Rundfunkrat (§ 49 WDR-Gesetz) sowie für das Deutschlandradio der Hörfunkrat und für das ZDF der Fernsehrat jeweils mit Zustimmung des Verwaltungsrats (§ 16 DRadio- bzw. § 16 ZDF-StV) bestellt. Meine Amtszeit ergibt sich aus dem jeweiligen Landesrundfunk- oder Landesmediengesetz bzw. dem Deutschlandradio- und dem ZDF-Staatsvertrag.

a Konstruktion

106 Das Amt der oder des Rundfunkdatenschutzbeauftragten besteht, wie insbesondere aus Art. 21 Abs. 1 S. 1 BR-Gesetz hervorgeht[51], unabhängig von der Umsetzungsentscheidung der für die Bestellung des Amtsinhabers jeweils verantwortlichen Gremien. In meinem Fall haben die Gremien sich gemeinsam auf einen Amtsinhaber und eine gemeinsam finanzierte Infrastruktur verständigt. Ein Vorbild für diese Konstruktion gibt es nicht. Auch deshalb wollen die beteiligten Gremien sie zu gegebener Zeit evaluieren.

[51] *„Es besteht ein Rundfunkdatenschutzbeauftragter."*

107 Der Rundfunkdatenschutzbeauftragte ist eine Aufsichtsbehörde im Sinne von Art. 51 DSGVO. Diese ist infolge der durch die DSGVO vorgegebenen Gewährleistungen völlig unabhängig von der Rundfunkanstalt und ihren Organen; insbesondere ist sie auch nicht etwa ein weiteres (viertes) Organ der Rundfunkanstalt. Nach der Entscheidung über die Besetzung der Position unterliegt sie nur noch einer eingeschränkten Dienstaufsicht und Finanzkontrolle durch den jeweiligen Verwaltungsrat, die in meinem Fall der Verwaltungsrat des Bayerischen Rundfunks für alle beteiligten Gremien federführend übernimmt. Ein auch nur mittelbarer Einfluss auf die Aufsicht etwa über die finanzielle oder personelle Ausstattung wird durch die gesetzlich zugewiesene Hoheit des Rundfunkdatenschutzbeauftragten über den Wirtschaftsplan und das Personal unterbunden.

108 Als Aufsichtsverantwortlicher ist der Rundfunkdatenschutzbeauftragte zugleich Amtsträger im öffentlich-rechtlichen und strafrechtlichen Sinne. Für die aufsichtsrechtliche Tätigkeit gelten neben den spezifischen Vorschriften der jeweiligen Rundfunkgesetze bzw. –staatsverträge die Verfahrensregelungen des Verwaltungsrechts. Im Einzelfall erlässt der Rundfunkdatenschutzbeauftragte daher auch förmliche Verwaltungsakte, die die Adressaten – sowohl Petenten wie auch Verantwortliche - gerichtlich überprüfen lassen können. Da sich mein Amtssitz in Potsdam-Babelsberg befindet, ist insoweit das Verwaltungsgericht Potsdam örtlich zuständig. Im Jahr 2019 war keiner meiner Bescheide Gegenstand eines Klagverfahrens.

109 Obwohl ich das Amt für fünf Rundfunkanstalten gemeinsam wahrnehme und nach Maßgabe einheitlicher gesetzlicher Vorgaben ausübe, ist dadurch im Rechtssinne nicht eine einheitliche Behörde entstanden. Vielmehr haben die verantwortlichen Gremien für die zur jeweiligen Rundfunkanstalt zu besetzende Funktion nur jeweils dieselbe Person gewählt. De iure repräsentiere ich mithin fünf Aufsichtsbehörden.

110 In organisationsrechtlicher wie praktischer Hinsicht ist diese Konstruktion mit einigen Nachteilen verbunden und bleibt deshalb hinter dem in meinen Augen eigentlich wünschenswerten und sinnvollen zurück. Das liegt jedoch nicht an den beteiligten Gremien. Denn eine eigenständige Datenschutzaufsichtsbehörde für einen Teil oder gar alle öffentlich-rechtlichen Rundfunkanstalten dürfte wegen der damit verbundenen organisationsrechtlichen Konsequenzen nur mit einer entsprechenden staatsvertraglichen Rahmenvorgabe der Länder wirksam institutionalisiert werden können. Da es eine solche zumindest bislang nicht gibt, ist die derzeitige Lösung immerhin ein pragmatischer Kompromiss, um gleichwohl einige mit der Zusammenführung der Aufsichtsfunktionen an einer Stelle verbundenen Vorteile zu generieren. Dies sind zum einen die Einsparungen, die sich daraus ergeben, dass nicht jede Rundfunkanstalt die Stellenkapazität für die – hauptamtlich wahrzunehmende – Funktion und das weitere Personal vorhalten muss, sondern sich lediglich an der Finanzierung der gemeinsamen Aufsicht beteiligt. Des weiteren befördert

dies ein einheitliches Verständnis der Anforderungen und vergleichbare Standards bei der Umsetzung der Datenschutzvorgaben sowie entsprechende Synergieeffekte. Und schließlich stärkt eine solche Konstruktion die Rolle und Wahrnehmung der Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk in der Öffentlichkeit.

b Organisation

111 Nicht nur die meinem Amt zugrunde liegende rechtliche Konstruktion ist aus den genannten Gründen singulär, sondern auch deren konkrete Ausgestaltung. Denn weder örtlich noch funktional bin ich einer der von mir zu beaufsichtigenden Rundfunkanstalten zugeordnet. Daher ist die durch die DSGVO bzw. die einschlägigen Landesgesetze vorgeschriebene strukturelle und funktionale Unabhängigkeit der Datenschutzaufsicht in meinem Fall zusätzlich administrativ und logistisch umfassend abgesichert. Auch dafür gab es kein Vorbild. Dies war und ist freilich wiederum mit einer Reihe rechtlicher und praktischer Umsetzungsfragen verbunden, die im Laufe des Jahres 2019 zu lösen waren.

112 Mein Amtssitz befindet sich in Potsdam-Babelsberg, und zwar in den Räumen der von den Mitgliedern der ARD und dem Deutschlandradio getragenen Stiftung Deutsches Rundfunkarchiv. Organisatorisch, administrativ und technisch betreut meine Aufsichtsbehörde jedoch der benachbarte Rundfunk Berlin-Brandenburg (rbb), für den (und dessen Vorgänger ORB) ich zuvor seit 1999 als Mitglied der Geschäftsleitung in unterschiedlichen Funktionen über viele Jahre verantwortlich tätig gewesen war. In datenschutzrechtlicher Hinsicht ist der rbb insoweit Auftragsverarbeiter, sodass ein entsprechender Vertrag zu vereinbaren war. Er sieht die strikte Trennung der für meine Aufsichtsbehörde zu verarbeitenden personenbezogenen Daten (sowohl in Bezug auf das Personal als auch hinsichtlich der Aufsichtstätigkeit) vom eigenen Bestand des rbb sowie angemessene technische und organisatorische Maßnahmen zum Schutz dieser Daten gegen unbefugten Zugriff (gleich ob von Seiten des rbb oder von Dritten) vor.

113 Diese Vorkehrungen wären auch dann erforderlich, wenn meine Aufsichtsbehörde organisatorisch einer der meiner Aufsicht unterliegenden Rundfunkanstalten zugeordnet wäre, wie dies sonst üblich ist. Im Falle des rbb sind sie aber zudem deshalb geboten, weil er zu jenen Rundfunkanstalten gehört, die - jenseits der Datenverarbeitung zu journalistischen Zwecken - der staatlichen Datenschutzaufsicht unterliegen (s.o. Rn. 91). Es muss deshalb ausgeschlossen sein, dass die Berliner Beauftragte für Datenschutz und Informationsfreiheit im (noch so unwahrscheinlichen) Fall einer Kontrolle des rbb auch auf die Daten meiner Aufsichtsbehörde zugreifen kann.

114 Selbstverständlich unterliegt meine Aufsichtsbehörde weder der Aufsicht noch der Kontrolle durch die Organe des rbb. Um zudem auch im Außenverhältnis den Eindruck zu vermeiden, es handele sich bei ihr womöglich um eine Stelle des rbb, soll weder die elektronische noch die telefonische Kommunikation mit diesem in Verbindung gebracht werden können. Daher war als eine der ersten Maßnahmen ein eigenständiger Mail-Account sowie eine eigene Telefondurchwahl einzurichten. Beides gelang erst nach einigen Schwierigkeiten, so wie auch die Nutzung eines elektronischen Aktenverwaltungssystems, das wir erst seit Ende des Jahres 2019 einsetzen können. Den eigenen, von einer Rundfunkanstalt unabhängigen Mail-Account konnte ich erst einrichten lassen, nachdem mir der Beitragsservice die bis dahin bei ihm angesiedelte, aber nie aktive Domain www.rundfunkdatenschutz.de übertragen hatte. Seit Ende März kann ich diese Webadresse als Plattform für die Darstellung und Kommunikation der wichtigsten Themen rund um meine Aufsichtsfunktion sowie als Kontaktportal für Beschwerdeführer und Verantwortliche nutzen.

115 Für die Aufsichtsbehörde sind bislang außer dem Rundfunkdatenschutzbeauftragten selbst eineinhalb weitere Planstellen (für eine/n Referent/in bzw. die gesetzlich vorgesehene Stellvertreterposition sowie das Sekretariat) geplant. Das Personal untersteht der ausschließlichen Verantwortung des Rundfunkdatenschutzbeauftragten. Dem Vernehmen nach hat selbst der Bundesdatenschutzbeauftragte bei der Gründung seiner Behörde mit 3 Stellen begonnen – freilich liegt das ziemlich genau 42 Jahre zurück, gewissermaßen in der „Steinzeit“ des Datenschutzes. Im Jahr 2014 waren daraus 85, bis 2019 bereits 250 Stellen geworden – und im Zusammenhang mit den infolge der DSGVO erheblich gestiegenen Anforderungen an die Datenschutzaufsicht hat der Bundestag dem Bundesbeauftragten in diesem Jahr sogar noch weitere 67 Stellen bewilligt, sodass die Bundesbehörde künftig 317 Stellen hat.

116 Natürlich ist dieser Vergleich nur bedingt aussagekräftig. Zumindest aber deutet er darauf hin, dass sich die personelle Ausstattung der gemeinsamen Datenschutzaufsicht in ihrem ersten Jahr gewiss am untersten Ende des gerade noch Vertretbaren bewegte. Dies stelle ich zunächst einmal nur fest, ohne es zu beklagen. Da (nicht nur den Gremien, sondern auch mir selbst) jegliche Erfahrungswerte in Bezug auf eine solche Konstruktion fehlten, und vor dem Hintergrund der mit ihr angestrebten Wirtschaftlichkeits- und Synergieeffekte sehe ich einen zurückhaltenden ersten Einstieg als durchaus legitim an. Sofern und sobald sich allerdings zeigt, dass die finanziellen oder personellen Ressourcen nicht mehr ausreichen, um wenigstens den Mindestbestand der gesetzlichen Aufgaben ordnungsgemäß wahrzunehmen, besteht zwingend Anpassungsbedarf. Ein solcher dürfte dann wiederum nicht etwa von einer einzelfallbezogenen vorherigen Genehmigung der Gremien oder gar der Rundfunkanstalten (bzw. ihrer Finanzabteilungen) abhängig gemacht werden. Dies wäre mit der Unabhängigkeit der Aufsichtsbehörde nicht vereinbar.

Die mit der personellen Situation verbundenen Risiken sind freilich durch ad hoc-Maßnahmen ohnehin nicht aufzufangen, da die spezifischen Aufgaben einer behördlichen Aufsicht temporären Vertretungs- bzw. Unterstützungslösungen durch Aushilfen o.ä. enge Grenzen setzen. Dies ist in Bezug auf die Stellen- und Personalausstattung in jedem Falle zu berücksichtigen.

c Zuständigkeit

117 Die Zuständigkeit meiner Aufsichtsbehörde ergibt sich aus den für mich jeweils maßgeblichen gesetzlichen bzw. staatsvertraglichen Regelungen. Neben den Rundfunkanstalten selbst sind dies zahlreiche von ihnen betreute sogenannte Gemeinschaftseinrichtungen sowie Beteiligungsunternehmen. Während letztere rechtlich selbstständig und deshalb in datenschutzrechtlicher Hinsicht eigenständig verantwortlich sind, nehmen für die rechtlich unselbstständigen Gemeinschaftseinrichtungen die an ihnen beteiligten Rundfunkanstalten bzw. ihre Intendantinnen und Intendanten diese Verantwortlichkeit gemeinsam wahr. Dem entspricht eine gemeinsame Zuständigkeit der Datenschutzaufsichtsbehörden der beteiligten Rundfunkanstalten; entsprechendes gilt für gemeinschaftliche Beteiligungsunternehmen mehrerer Rundfunkanstalten. Es liegt auf der Hand, dass eine solche gemeinsame Aufsichtstätigkeit zu erheblichem Koordinations- und Abstimmungsaufwand führen würde, der durch ein Federführungsprinzip vermeidbar ist. Rechtssicher umsetzbar ist ein solches nur durch entsprechende Verwaltungsvereinbarungen aller beteiligten Aufsichtsbehörden, für die ich mich daher frühzeitig eingesetzt habe. Ich erwarte, dass sie im Laufe des Jahres 2020 zustande kommen.

118 Eine Übersicht über die rechtlich unselbstständigen Einrichtungen und Beteiligungsunternehmen in meinem Zuständigkeitsbereich ist auf meiner Homepage veröffentlicht[52]. Zu ihnen gehört unter anderem der Beitragsservice von ARD, ZDF und Deutschlandradio, soweit es um die datenschutzrechtlichen Anforderungen an die Organisation vor Ort sowie Fragen des Datenschutzes im Verhältnis zu den Beitragszahlerinnen und Beitragszahlern aus den Sendegebieten von BR, SR und WDR geht; im übrigen sind die Datenschutzaufsichten der anderen Landesrundfunkanstalten zuständig, darunter – im Falle des HR, RB und rbb – auch die Landesdatenschutzbehörden aus Berlin/Brandenburg, Bremen und Hessen. Wenig überraschend, bezieht sich ein erheblicher Anteil der bei mir eingehenden Anfragen und Beschwerden auf den Beitragsservice (s. unten Rn. 149 ff.).

119 Darüber hinaus erstreckt sich meine Aufsichtszuständigkeit auch auf alle Auftragsverarbeitungsverhältnisse der betreffenden Rundfunkanstalten. Dies hat

52 https://www.rundfunkdatenschutz.de/ueber-uns/aufsicht-ueber-sonstige-einrichtungen-und-beteiligungsunternehme.html

2019 im Einzelfall zu rechtlichem wie auch praktischem Klärungsbedarf geführt. Auch insoweit hat die DSGVO neue Fragen aufgeworfen (s. dazu auch unten Rn. 219 ff.).

d Aufgaben und Tätigkeit

120 Meine Aufgaben ergeben sich unmittelbar aus dem umfangreichen Katalog des Art. 57 Abs. 1 DSGVO sowie den für mich maßgeblichen landesgesetzlichen bzw. staatsvertraglichen Vorschriften. Nicht nur angesichts der bereits angesprochenen knappen Ressourcen wäre es nicht annähernd realistisch, sich in der Praxis an diesem umfassenden Aufgabenspektrum zu orientieren. Für die praktische Umsetzung sind für mich daher zwei Leitlinien maßgeblich:

121 Dies ist zum einen die klare Fokussierung und Beschränkung auf eine Aufsichtsfunktion im engeren Sinne. Dies legt schon das bereits angesprochene Leitbild der DSGVO nahe (oben Rn. 19) , das auch daran erkennbar wird, dass – anders als noch nach früherem deutschem Recht - eine Beratungsaufgabe der Aufsicht im Verhältnis zum Verantwortlichen nicht mehr explizit vorgesehen ist. Sie soll vielmehr ganz bewusst und nach Maßgabe der insoweit ihrerseits gestärkten unabhängigen Position primär der interne Datenschutzbeauftragte nach Art. 37 DSGVO übernehmen. Dies schließt keineswegs aus, dass sich der Verantwortliche oder jeweilige Datenschutzbeauftragte im Einzelfall zu Beratungszwecken an den Rundfunkdatenschutzbeauftragten wendet, vgl. Art. 57 Abs. 1 lit. v) DSGVO. Aber es handelt sich dann um eine freiwillige Aktivität der Aufsicht nach Maßgabe ihrer Kapazitäten. Daher bieten auch die staatlichen Datenschutzbehörden aus Kapazitätsgründen eine Beratung inzwischen – wenn überhaupt – überwiegend nur noch eingeschränkt an. Diese Maßgabe spiegelt auch mein Tätigkeitsbericht wider, in dem ich ausschließlich auf jene Themen eingehe, die für mich 2019 unmittelbar aufsichtsrechtlich relevant waren.

122 Zum anderen kann ich naturgemäß nur jene Aufgaben wahrnehmen, die mit den verfügbaren personellen, finanziellen und zeitlichen Kapazitäten zu bewältigen sind. Im Mittelpunkt steht dabei die Reaktion auf alle Kontakte im Außenverhältnis, vor allem in Gestalt von an mich gerichteten Beschwerden. Anders als den Rundfunkanstalten selbst kann ich mich insoweit auch nicht ohne weiteres durch einen externen Dienstleister unterstützen lassen oder sogar bestimmte Teilaufgaben delegieren, da dies im Bereich der hoheitlichen Tätigkeit nur sehr eingeschränkt zulässig ist (s.o. Rn. 115 f.).

123 Mit unterschiedlichen zeitlichen Anteilen richte ich mein Hauptaugenmerk vor diesem Hintergrund auf die folgenden, mir zugewiesenen Aufgaben nach Art. 57 Abs.

1 DSGVO; nur einigen davon wiederum habe ich mich im Jahr 2019 tatsächlich vertieft widmen können:

- Anwendung DSGVO überwachen und durchsetzen (lit. a)
- Öffentlichkeit, insbes. Kinder sensibilisieren und aufklären (lit. b)
- Verantwortliche und Auftragsverarbeiter sensibilisieren (lit. d)
- Betroffene Personen über ihre Rechte aufklären (lit. e)
- Beschwerden nachgehen (lit. f)
- Zusammenarbeit anderen Aufsichtsbehörden (lit. g)
- Untersuchungen über Anwendung der DSGVO durchführen (lit. h)
- maßgebliche Entwicklungen verfolgen (lit. i)
- Liste der Anwendungen anlegen, die eine DSFA erfordern (lit. k).

e Befugnisse

124 Da die Funktion des Rundfunkdatenschutzbeauftragten die einer Aufsichtsbehörde nach Art. 51 DSGVO ist, übertragen die für mich maßgeblichen landesrechtlichen Regelungen mir konsequenterweise auch die Befugnisse „entsprechend Art. 58 Abs. 1 bis 5 DSGVO." Dies umfasst Befugnisse auf Untersuchungen (Abs. 1) und Abhilfe (Abs.2) gegenüber den Verantwortlichen und ihren Auftragsverarbeitern sowie die in Abs. 3 enumerativ genannten Genehmigungs- und Beratungsbefugnisse. Die Abhilfeoptionen nach Abs. 2[53] unterteilen sich in retrospektiv-sanktionierende und prospektiv-verhaltenssteuernde Reaktionen. Zur zweiten Fallgruppe zählen die (vorbeugende) Warnung (lit. a) sowie unterschiedliche Anweisungen (lit. c – e), zur ersten neben der Verwarnung (lit. b) als mildestem Mittel unter anderem die Anordnung, eine Datenverarbeitung ganz oder teilweise zu berichtigen, zu löschen oder einzuschränken (lit. g) oder die Geldbuße (lit. i iVm. Art. 83 DSGVO); diese kann auch neben anderen Maßnahmen verhängt werden.

125 Die Sanktionierung der Rundfunkanstalten durch ein Bußgeld allerdings schließen die für mich maßgeblichen landesrechtlichen Regelungen explizit aus[54]. Dabei handelt es sich nur vordergründig um eine Privilegierung der Rundfunkanstalten. Denn dies entspricht dem allgemeinen Grundsatz, dass finanzielle Sanktionen gegenüber von der Allgemeinheit finanzierten öffentlich-rechtlichen Institutionen nicht sinnvoll sind, würden sie letztlich doch nur den Etat schmälern, aus dem die Einrichtung just die im öffentlichen Interesse liegenden Aufgaben zu finanzieren hat. Stattdessen sehen die rundfunkrechtlichen Regelungen jedoch mit dem Instrument der förmlichen Beanstandung eine spezifische Sanktion vor, die im allgemeinen Daten-

[53] Siehe dazu auch Kurzpapier Nr. 2 der DSK, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_2.pdf

[54] Art. 21 Abs. 6 S. 3 BR-G, § 42d Abs. 1 S. 4 SMG, § 51 Abs. 1 S. 4 WDR-G, § 18 Abs. 1 S. 4 DRadio- bzw. ZDF-StV.

schutzrecht nicht zur Verfügung steht[55]. Danach beanstandet der Rundfunkdatenschutzbeauftragte von ihm festgestellte Verstöße gegen Datenschutzvorschriften oder sonstige Mängel bei der Verarbeitung personenbezogener Daten gegenüber dem Intendanten und fordert ihn zu einer Stellungnahme innerhalb einer angemessenen Frist auf; gleichzeitig unterrichtet er den Verwaltungsrat. Von beidem kann er absehen, wenn es sich um unerhebliche Mängel handelt oder wenn ihre unverzügliche Behebung sichergestellt ist.

126 Der Wortlaut dieser Regelung könnte eine Interpretation nahelegen, nach der sich die Sanktionsbefugnisse des Rundfunkdatenschutzbeauftragten nur auf die förmliche Beanstandung beschränken. Dies ließe sich allerdings mit dem ausdrücklichen Hinweis auf die Maßnahmen gemäß Art. 58 Abs. 1 bis 5 DSGVO nicht vereinbaren. Nach meinem Verständnis ist die förmliche Beanstandung gegenüber dem Intendanten mit den damit verbundenen Informations- und Verfahrensmechanismen vielmehr das Äquivalent zur Geldbuße. Wie diese kann die Beanstandung deshalb nicht nur als ultima ratio, sondern im Einzelfall auch zusätzlich zu den Maßnahmen nach Art. 58 Abs. 1 bis 3 DSGVO ausgesprochen werden.

127 Unberührt vom Ausschluss der Geldbuße gegenüber den Rundfunkanstalten bleibt die Möglichkeit, eine solche bei entsprechend schwerem Fehlverhalten gegenüber einzelnen Beschäftigten der Rundfunkanstalt zu verhängen. Und unberührt bleibt außerdem die entsprechende Sanktionsbefugnis gegenüber den Beteiligungsunternehmen der Rundfunkanstalten sowie den jeweiligen Auftragsverarbeitern.

128 Einen Anlass zu einer förmlichen Beanstandung bzw. zur Verhängung eines Bußgelds habe ich im Jahr 2019 nicht gesehen. In einigen Fällen musste ich eine Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO aussprechen, in anderen Maßnahmen nach Art. 58 Abs. 2 lit. d) DSGVO anordnen bzw. festhalten. Zu Auseinandersetzungen kam es dabei nicht. Durchweg haben die Verantwortlichen sich kooperativ gezeigt und umgehend reagiert.

f Zusammenarbeit mit anderen Stellen

aa) Öffentlich-rechtlicher Rundfunk

129 Eine enge Zusammenarbeit der für die **Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk** Zuständigen ist – unabhängig von der (allerdings unmittelbar nur für die europaweite Zusammenarbeit maßgeblichen) generellen Vorgabe des Art. 60 DSGVO – schon deshalb sinnvoll und geboten, weil die Rundfunkanstal-

[55] Art. 21 Abs. 7 und 8 BR-G, § 42d Abs. 2 bis 4 SMG, § 52 Abs. 2 bis 4 WDR-G, § 18 Abs. 2 und 3 DRadio- bzw. ZDF-StV

ten sowohl publizistisch als auch administrativ und organisatorisch in vielfältiger Weise miteinander kooperieren und gemeinsame Einrichtungen und Beteiligungsgesellschaften halten. Viele Projekte und Vorgänge betreffen deshalb von vornherein mehrere oder sogar alle Rundfunkanstalten in gleicher Weise, so dass eine einheitliche datenschutzrechtliche Bewertung erforderlich ist, weil es letztlich um die datenschutzrechtlichen Konsequenzen für das „System öffentlich-rechtlicher Rundfunk" geht. Dies wird freilich erschwert durch die bereits angesprochenen (s.o. Rn. 30) uneinheitlichen Aufsichtskonstruktionen und -zuständigkeiten in Bezug auf die einzelnen Rundfunkanstalten.

130 Frühzeitig habe ich mich vor diesem Hintergrund für die Einrichtung einer **Rundfunkdatenschutzkonferenz (RDSK)** eingesetzt, in der ausschließlich die für die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk zuständigen Stellen vertreten sind. Sie hat sich im Mai 2019 konstituiert. Zu ihren Aufgaben gehört es, gemeinsame Kriterien und Standards im Datenschutz zu entwickeln sowie Positionen zu wichtigen datenschutzrechtlichen Fragen zu entwickeln, die den öffentlich-rechtlichen Rundfunk betreffen. Das Ziel muss dabei eine strikte Fokussierung auf die im engeren Sinne aufsichtsrechtlichen Themen sein, verbunden mit einer strengen Kommunikation im Verhältnis zu den jeweiligen Verantwortlichen und gegenüber der Öffentlichkeit. Eine Geschäftsordnung regelt die wichtigsten Fragen zur Verständigung im Wege von Beschlüssen, Entschließungen oder Empfehlungen, für die grundsätzlich Einvernehmen angestrebt wird. Das Verfahren im einzelnen wie auch die Agenda muss sich im Laufe der Zeit noch herausbilden. Künftig sollen alle wichtigen Themen der RDSK auch auf einer eigenen Homepage veröffentlicht werden.

131 Darüber hinaus tauschen sich die meisten Mitglieder der RDSK und die internen Datenschutzbeauftragte aller Rundfunkanstalten, mehrerer Gemeinschaftseinrichtungen sowie von Arte und ORF in dem bereits seit Mitte der 1980er Jahre bestehenden Arbeitskreis der Datenschutzbeauftragten (**AKDSB**) über Fragen und Themen aus, die die Rundfunkanstalten gemeinsam betreffen. Er tagt in der Regel zweimal jährlich und erörtert sämtliche Fragen des „operativen Datenschutzes". Insbesondere kann er dazu bestimmte einheitliche Empfehlungen an die Verantwortlichen entwickeln und so darauf hinwirken, dass alle Institutionen gleiche Datenschutzstandards einhalten. Dies ist besonders wichtig für große IT-Infrastrukturprojekte oder alle Anwendungen, mithilfe derer die Rundfunkanstalten personenbezogene Daten gemeinsam verarbeiten bzw. einander übermitteln.

132 Dem AKDSB gehören auch die Datenschutzbeauftragten der fünf Rundfunkanstalten in meinem Zuständigkeitsbereich sowie die behördliche DSB des Beitragsservice von ARD, ZDF und Deutschladradio sowie ihre jeweiligen Stellvertreter an. Unter anderem mit Blick auf ihre eigenständige, unabhängige Funktion, um unnötige Überschneidungen und Abstimmungsaufwand im Binnenverhältnis zu mir zu ver-

meiden sowie aus Kapazitätsgründen habe ich mich entschieden, mich am AKDSB nicht zu beteiligen. Stattdessen habe ich einen zweimal jährlichen Austausch mit dem kleineren Personenkreis der Datenschutzbeauftragten meines Zuständigkeitsbereichs in einer sogenannten 5+1-Runde angeboten, der sich als sehr fruchtbar erwiesen hat und deshalb auf Wunsch aller Beteiligten fortgesetzt werden soll. In ähnlicher Weise pflegen auch die staatlichen Aufsichtsbehörden den Kontakt mit den behördlichen oder betrieblichen Datenschutzbeauftragten ihres jeweiligen Zuständigkeitsbereichs.

133 Zudem habe ich im Laufe des Jahres 2019 die Datenschutzbeauftragten etlicher Gemeinschaftseinrichtungen und Beteiligungsunternehmen in meinem Zuständigkeitsbereich besucht und ihnen im Bedarfsfall meine Unterstützung angeboten. Wenig überraschend zeigte sich, dass sie vielfach mit denselben Themen bzw. Vorhaben befasst sind wie die Datenschutzbeauftragten der Rundfunkanstalten, so etwa die Zulässigkeit und die Rahmenvorgaben für die Nutzung von Cloudanwendungen oder den Einsatz von Bürosoftware wie Office 365. Insofern möchte ich weitere Möglichkeiten ausloten, diesen Personenkreis in den allgemeinen Informations- und Erfahrungsaustausch einzubeziehen.

bb) Andere Aufsichtsstellen

134 Daneben habe ich frühzeitig den Kontakt zu anderen Aufsichtsstellen gesucht, um mein Interesse an einer konstruktiven Zusammenarbeit zu signalisieren und meinerseits eine solche anzubieten.

135 Besonders bedeutsam ist bzw. wäre ein enger Austausch naturgemäß mit den unabhängigen **staatlichen Datenschutzbehörden**. Dafür spricht schon die große Zahl thematischer und funktionaler Überscheidungen im jeweiligen Zuständigkeitsbereich. Das erklärte Ziel der DSGVO ist eine einheitliche Durchsetzung der sich aus ihr ergebenden Datenschutzvorgaben durch alle Aufsichtsbehörden. Zuverlässig und umfassend zu gewährleisten wäre dies über ein gemeinsames Gremium sämtlicher unabhängiger nationaler Aufsichtsbehörden, zu denen außer den staatlichen Stellen und den Rundfunk- bzw. Mediendatenschutzbeauftragten auch die kirchlichen Datenschutzbeauftragten gehören. Dafür müsste die von Seiten der staatlichen Behörden gegründete Datenschutzkonferenz (DSK) freilich um diesen Kreis erweitert oder gegebenenfalls ein Alternativmodell entwickelt werden, in dem die jeweiligen Gruppen durch einzelne Aufsichtsbehörden vertreten sind. Allerdings sträuben sich einzelne Mitglieder der DSK – und damit im Ergebnis diese insgesamt - gegen eine derartige institutionalisierte Verbindung mit den Rundfunkdatenschutzbeauftragten bzw. weiteren Aufsichtsbehörden oder auch nur eine engere inhaltliche Abstimmung mit diesen. Die dafür mitunter genannten Gründe fußen erkennbar teilweise noch auf den tradierten Vorbehalten gegen die Unabhängigkeit

der Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk und sind weder insoweit noch im übrigen wirklich stichhaltig.

136 Vordergründig kann sich die DSK auch auf die schon oben (Rn. 21) problematisierte Vorschrift des § 18 Abs. 1 S. 4 BDSG zurückziehen, die eine Abstimmung zwischen ihren Mitgliedern und den nach Art. 85 und 91 DSGVO eingerichteten sogenannten „spezifischen Aufsichtsbehörden" lediglich in Bezug auf „Angelegenheiten der EU mit dem Ziel einer einheitlichen Anwendung der DSGVO" und nur insoweit fordert, als diese „von der Angelegenheit betroffen sind." Nach ihrer Auffassung steht deshalb jede darüber hinausgehende Einbeziehung etwa der Rundfunkdatenschutzbeauftragten bzw. Mitglieder der RDSK in Themen zur Umsetzung der DSGVO im freien Belieben der DSK bzw. ihrer Mitglieder.

137 Die einseitige Vorgehensweise der staatlichen Datenschutzaufsichten liefert ein Anschauungsbeispiel für die normative Kraft des Faktischen, ist sie doch letztlich Ausdruck des erheblichen Ungleichgewichts in Bezug auf die für die Aufsicht jeweils zur Verfügung stehenden Ressourcen. Unbeschadet dessen halte ich es allerdings weder für erstrebenswert noch für erforderlich, die DSK durch ein Gremium zu ersetzen, das sämtliche Aufsichtsbehörden umfasst. Nicht nur wäre ein derart großer Kreis kaum arbeitsfähig, sondern natürlich behandelt die DSK trotz zahlreicher Überschneidungen auch viele Themen, die jedenfalls für meine Aufsichtspraxis nicht oder nicht prioritär relevant sind.

138 Sehr wohl halte ich aber eine strukturierte Zusammenarbeit und Abstimmung über das durch die DSK einseitig festgelegte Maß hinaus für angezeigt und geboten. Insoweit besteht zwischen den Aufsichtsbehörden nicht etwa ein Subordinations-, sondern ein Gleichordnungsverhältnis. Nach dem Verständnis des Rechtsstaatsprinzips und des deutschen Organisationsverfassungsrechts erfordert dies ein wechselseitiges Verfahren auf Augenhöhe.

139 Immerhin hat es im Jahr 2019 erste Anzeichen einer vorsichtigen Öffnung der DSK gegeben, die sich bereitgefunden hat, sich regelmäßig zweimal jährlich mit den „spezifischen" Aufsichtsstellen auszutauschen[56]. Bislang legt die DSK diese Runde allerdings eher retrospektiv-informierend als auf eine inhaltliche Zusammenarbeit oder einen frühzeitigen Meinungsaustausch zu bestimmten Themen an. Daneben hat sie sich aber immerhin bereit erklärt, eine Vertretung der RDSK an den Arbeitskreisen der DSK zu ermöglichen. Auf dieser Grundlage habe ich 2019 an einer Sitzung des AK Grundsatzfragen teilgenommen, in der es im wesentlichen um den Bericht der DSK zur Evaluation der DSGVO ging. Außerdem war die RDSK

[56] S. dazu Beschluss der DSK vom 13.5.2019 (Punkt 8): https://www.datenschutzkonferenz-online.de/media/dskb/20190513_dskb_beteiligung_ab.pdf

in einer Sitzung des AK Technik durch die Datenschutzbeauftragte von Radio Bremen bzw. meine Referentin vertreten. Und schließlich habe ich mein Interesse an einer Mitwirkung im AK Datenschutz-/Medienkompetenz bekundet, an dessen Sitzung ich allerdings noch nicht teilnehmen konnte.

140 Durchweg akzeptieren die Arbeitskreise der DSK eine Beteiligung von Vertretern der RDSK jeweils nur im Rahmen eines „Gaststatus". Dies ist grundsätzlich nachvollziehbar, da es sich „nur" um Untergruppierungen der DSK handelt, der die Rundfunkdatenschutzbeauftragten nicht angehören. Dass daraufhin den Vertretern der RDSK im Vorfeld allerdings weder die Tagesordnung noch gar Sitzungsunterlagen zur Verfügung gestellt wurden, unterläuft letztlich den Sinn und Zweck einer Teilnahme und ist alles andere als der Ausdruck eines respektvollen Umgangs auf Augenhöhe. Auch dies soll künftig aber offenbar anders gehandhabt werden.

141 Insgesamt ist hier also noch viel Luft nach oben. Dies umso mehr, als es nach meiner Überzeugung das System der Datenschutzaufsicht in Deutschland insgesamt stärken würde, wenn sich die staatlichen Datenschutzaufsichten auf eine engere Zusammenarbeit einließen und auf diesem Weg auch die unterschiedlichen Erfahrungen und Expertise insbesondere der Mitglieder der RDSK und der kirchlichen Aufsichtsbehörden nutzen würden.

142 Vor diesem Hintergrund ist bislang auch noch völlig unklar, ob und wie die DSK die Rundfunkdatenschutzbeauftragten in die Agenda des Europäischen Datenschutzausschusses einbeziehen werden. Art. 63 DSGVO unterscheidet in Bezug auf das europäische Kohärenzverfahren jedenfalls nicht nach Aufsichtsstellen unterschiedlicher Kategorie. Zwar lässt Art. 85 Abs. 2 DSGVO insoweit auch Ausnahmeregelungen auf nationaler Ebene zu – allerdings nur, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen. Davon kann im Falle einer Einschränkung von Beteiligungs- bzw. Verfahrensrechten der Rundfunkdatenschutzbeauftragten sicher nicht die Rede sein (s. schon oben Rn. 21 f.).

143 Unbeschadet dessen habe ich im Laufe des Jahres 2019 den Kontakt zu einzelnen Landesdatenschutzbeauftragten und weiteren Aufsichtsorganisationen gesucht. Von besonderem Interesse waren insoweit für mich Gespräche mit den Vertretern der **Datenschutzaufsicht der Kirchen**, hier dem Datenschutzbeauftragten der EKD sowie dem letztjährigen Vorsitzenden der Konferenz der Diözesandatenschutzbeauftragten. Dabei ging es mir weniger um inhaltliche Fragen des Datenschutzes als vielmehr um die Konstruktion der Datenschutzaufsicht in den beiden großen Kirchen. Denn diese sind mit ihren komplexen Strukturen sowie wegen ihres verfassungsrechtlichen Sonderstatus' in mancherlei Hinsicht der ARD (bzw. dem System des öffentlich-rechtlichen Rundfunks) vergleichbar. Daher standen (und stehen) auch die Kirchen vor der Herausforderung, eine effiziente und effek-

tive Datenschutzaufsicht zu etablieren und haben dafür stringente rechtliche Rahmenbedingungen entwickelt: In beiden Systemen ist die Aufsicht auf übergeordneter Ebene (in der Form einer Körperschaft des öffentlichen Rechts) organisationsrechtlich verselbstständigt, die Katholische Kirche unterhält sogar eine eigenständige Datenschutzgerichtsbarkeit.

144 Im Mittelpunkt meines Austauschs mit der **Geschäftsstelle des Deutschen Presserats** standen hingegen Fragen zur Praxis der Datenschutzaufsicht im Bereich der Presse und der von den Verlagen veranstalteten Telemedien. Dass die betreffenden Unternehmen es selbst in der Hand haben, über die Aufsicht über ihre Angebote zu entscheiden, indem sie sich dem Deutschen Presserat anschließen, ist im System der deutschen Aufsichtskonstruktion durchaus ungewöhnlich.

145 Und schließlich habe ich an einem Treffen der Projektpartner des sogenannten **Virtuellen Datenschutzbüros** teilgenommen, das sich als gemeinsame Informationsplattform aller beteiligten Datenschutzaufsichtsstellen für die Öffentlichkeit versteht. Die Geschäftsführung dieser Einrichtung hat das Datenschutzzentrum Schleswig-Holstein inne. Über die von ihm betreute Homepage werden unter anderem auch meine Tätigkeitsberichte abrufbar sein.

146 Wünschenswert wäre darüber hinaus vor dem Hintergrund der entsprechenden Zielsetzung der DSGVO eine Zusammenarbeit bzw. ein Austausch über Fragen des medienspezifischen Datenschutzes mit den für den Rundfunk zuständigen **Aufsichtsbehörden auf europäischer Ebene**. Die EBU hat zwar mit der Data Protection Officers Group (in der ARD/WDR und ZDF durch je eine Kollegin vertreten sind) sowie der Data Protection Interdisciplinary Group zwei Arbeitsgruppen eingerichtet, die sich mit Datenschutz- bzw. datenschutzrechtlichen Themen befassen. Dort geht es jedoch ausschließlich um Fragen zum Verständnis und zur Umsetzung der DSGVO auf operativer Ebene. Da eine autonome Datenschutzaufsicht wie im deutschen öffentlich-rechtlichen Rundfunk ansonsten in der EBU nicht bekannt, zumindest aber nicht organisiert ist, fehlt auf der Ebene der Rundfunkdatenschutzbeauftragten dort jeweils ein Pendant. Leider gibt es bislang auch keine Übersicht über die Aufsichtszuständigkeiten in den anderen EU-Mitgliedstaaten in Bezug auf Rundfunk und Telemedien, sodass einer entsprechenden Kontaktaufnahme noch einige Recherchen vorangehen müssten. Da mir gerade im ersten Jahr meiner Amtszeit anderes vordringlich schien, musste ich konkrete Bemühungen in dieser Hinsicht deshalb einstweilen zurückstellen.

147 Auch für sonstige Aktivitäten jenseits der Aufsichtsfunktion im engeren Sinne, namentlich den Besuch einschlägiger **Veranstaltungen**, blieb wenig Zeit. Immerhin konnte ich mir auf dem jährlichen Datenschutzkongress in Berlin im Mai einen Überblick über den aktuellen Diskussions- und Erkenntnisstand zur Umsetzung der DSGVO verschaffen. Daneben habe ich drei von der Stiftung Datenschutz – eben-

falls jeweils in Berlin – organisierte Podiumsdiskussionen, ein internationales Symposion in Potsdam sowie zwei datenschutzrechtliche Tagungen in Mainz und München besucht.

4 Schwerpunktthemen der eigenen Praxis

148 Aus der Vielzahl unterschiedlichster Vorgänge, mit denen ich in meiner Aufsichtspraxis befasst war, gehe ich im folgenden nur auf diejenigen ein, in denen es zumindest auch um Fragen grundsätzlicher Natur ging.

a Auskunftsverfahren

149 Bei weitem die meisten aller bei mir eingegangen Anfragen und Beschwerden betrafen das Recht auf Auskunft gemäß Art. 15 DSGVO. Davon entfiel wiederum der mit Abstand größte Anteil auf den Beitragsservice von ARD, ZDF und Deutschlandradio. Freilich löste nur ein Teil davon aufsichtsrechtliche Verfahren aus: Häufig hatten die Petenten verkannt, dass sich der Anspruch nicht an die Aufsicht, sondern an den jeweils Verantwortlichen richtet, an den ich insoweit dann verwiesen habe. Entsprechendes galt für mehrere Beschwerden von Rundfunkteilnehmern außerhalb meines Zuständigkeitsbereichs, die ich an das jeweilige RDSK-Mitglied verwiesen habe.

150 In etlichen Fällen allerdings ging es darum, dass der Beitragsservice auf ein formell ordnungsgemäß an ihn gerichtetes Auskunftsbegehren nicht innerhalb der **Frist** des Art. 12 Abs. 3 DSGVO reagiert hatte. Es stellte sich heraus, dass für entsprechende Verzögerungen typischerweise zwei Faktoren ursächlich waren: Zum einen hatte die Entscheidung des BVerfG vom 18. Juli 2018 zur Befreiung von Nebenwohnungen vom Rundfunkbeitrag zu einem massiv gestiegenen Korrespondenzaufkommen und infolgedessen zu einem erheblichen Bearbeitungsstau geführt, der sich auch auf diese Vorgänge auswirkte. Zum anderen hatten die Petenten ihren Auskunftsanspruch in den betreffenden Fällen durchweg nicht ohne weiteres erkennbar, sondern im Rahmen eines „normalen“ Beitragsverfahrens beispielsweise erst am Ende eines viele Seiten umfassenden Schriftstücks formuliert.

151 Bei der Bewertung war zu berücksichtigen, dass der Beitragsservice ein enormes Korrespondenzaufkommen zu bewältigen hat und dafür aus wirtschaftlichen Gründen – also insbesondere im Interesse der Beitragszahler – in größerem Umfang automatisierte Verfahren zur Erfassung und Zuordnung von Posteingängen einsetzt. Um den technischen, zeitlichen und finanziellen Aufwand weiter zu begrenzen, war die automatisierte Datenerfassung ursprünglich nicht auf das gesamte jeweils eingehende Schriftstück, sondern einen Teil beschränkt. Dies genügte, um alle beitragsrechtlichen Vorgänge ordnungsgemäß zu erfassen und intern zuzuordnen.

Nach dem Inkrafttreten der DSGVO und dem Anstieg der auf ihrer Grundlage geltend gemachten Ansprüche hat sich die Situation jedoch verändert, da nun neben den beitrags- auch datenschutzrechtliche Belange und Fristen zu beachten sind. Der Beitragsservice hat auf meine Veranlassung hin inzwischen mit einer Reihe von organisatorischen und technischen Vorkehrungen reagiert, die seither eine fristgerechte Bearbeitung auch atypischer Auskunftsersuchen oder sonstiger datenschutzrechtlicher Vorgänge gewährleisten sollen.

152 In einigen Fällen monierten Beschwerdeführer, dass die ihnen erteilte Auskunft nicht **vollständig** gewesen sei. Ursache dafür ist die Entscheidung des Beitragsservice, Auskünfte grundsätzlich im Rahmen eines zweistufigen Verfahrens zu erteilen: Die Erstauskunft umfasst die wichtigsten Informationen über die Umstände der Datenverarbeitung wie etwa die Herkunft der Daten, die Datenverarbeitungskategorien und die Verarbeitungszwecke. Inhaltlich erstreckt sie sich auf alle aktuellen Daten, die gemäß § 8 Abs. 4 RBStV anzuzeigen und daher schon qua Gesetz als besonders relevant qualifiziert sind. Darüber hinaus umfasst sie Angaben zu Befreiungen bzw. Ermäßigungen sowie - im Falle eines Lastschrifteinzugs - Daten zur Bankverbindung. In den weitaus meisten Fällen genügt den Antragstellern die auf diese Angaben beschränkte Erstauskunft des Beitragsservice. Dieser ergänzt sie in allen anderen Fällen unverzüglich um die Mitteilung der etwa vorhandenen weiteren Daten, sofern die Antragsteller dies wünschen.

153 Ein solches zweistufiges Verfahren, das nicht zuletzt den Verwaltungsaufwand deutlich reduziert und damit im Interesse aller Beitragszahler unnötige Kosten vermeidet, erfüllt sowohl den Sinn und Zweck als auch materiell die Anforderungen des Art. 15 DSGVO. Dass Aspekte der Verhältnismäßigkeit bzw. des vertretbaren Aufwands in die Anwendung bzw. Umsetzung der Vorgaben zum Auskunftsanspruch nach Art. 15 DSGVO einfließen können, geht aus EG 63 DSGVO sowie Vorschriften wie etwa § 34 Abs. 1, 4 BDSG, § 12 Abs. 1 LDSG NRW, Art. 10 Abs. 2 Nr. 4 und 5 BayDSG oder § 9 Abs. 2 LDSG B-W hervor. Dabei ist insbesondere zu berücksichtigen, dass der Beitragsservice einen außerordentlich großen Datenbestand zu verwalten und dabei auf ein Höchstmaß an Effizienz, Wirtschaftlichkeit und Sparsamkeit zu achten hat, vgl. § 14 RStV. Das Recht auf Auskunft wird weder inhaltlich beschränkt noch unzumutbar erschwert, da der Beitragsservice hinreichend klar auf das abgestufte Verfahren und das Recht des Betroffenen hinweist, die Auskunft vervollständigen zu lassen.

154 Schließlich hatte ich mich auch noch mit der Forderung zu befassen, neben der Auskunft nach Art. 15 Abs. 1 noch eine vollständige **Aktenkopie** zu erhalten. Gestützt wird ein solcher Anspruch auf die Vorschrift des Art. 15 Abs. 3 DSGVO, nach der der Verantwortliche auf entsprechendes Verlangen „eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung“ stellt. Die Reichweite dieser Vorschrift ist sowohl in Literatur und Rechtsprechung als auch

bei den Datenschutzaufsichtsbehörden umstritten. Nach meiner Überzeugung lässt sich ein derart weitgehender Anspruch aus ihr jedenfalls für den Regelfall[57] nicht ableiten:

155 Schon nach ihrem Wortlaut bezieht sich die Vorschrift nur auf die personenbezogenen Daten selbst, nicht hingegen auf die jeweiligen Datenträger und/oder Datensätze, auf bzw. in denen sich diese Daten befinden. Der Sache nach geht es dabei um eine Zusammenstellung sämtlicher Daten, die der Verantwortliche über die betroffene Person verarbeitet, unabhängig davon, in welcher Form, in welcher Gestalt und auf welchem Medium dies geschieht. Eine Kopie dieser Übersicht hat der Verantwortliche zur Verfügung zu stellen.

156 Diese Interpretation entspricht auch dem Sinn und Zweck der Vorschrift. Sie soll gegenüber dem Betroffenen Transparenz darüber herstellen, welche Daten der Verantwortliche zu seiner Person verarbeitet, und ihm auf diese Weise beispielsweise die Wahrnehmung seiner Rechte nach den Artt. 16 ff. DSGVO erleichtern. Die entsprechende Übersicht muss daher die personenbezogenen Daten vollständig, aktuell und unverändert exakt so ausweisen, wie sie der Verantwortliche verarbeitet. Dagegen ist der Betroffene für die Geltendmachung seiner weiteren Ansprüche nach den Artt. 16 ff. DSGVO nicht darauf angewiesen, zu erfahren, auf welchen einzelnen Datenträgern oder in welchen Datensätzen seine personenbezogenen Daten jeweils verarbeitet werden.

157 Zudem steht es im Widerspruch zu dem Art. 15 DSGVO zugrunde liegenden Transparenzanspruch, wenn der Verantwortliche anstelle einer solchen Übersicht einfach eine Kopie sämtlicher Datenträger zu übersenden hätte, auf denen sich die personenbezogenen Daten befinden. Denn in diesem Fall müsste sich der Betroffenen selbst den entsprechenden Überblick verschaffen. Abgesehen davon liefe ein derart weitreichendes Verständnis der Vorschrift auf einen Anspruch auf Überlassung des vollständigen Verwaltungsvorgangs hinaus und ginge damit noch weiter als ein nach den einschlägigen Verwaltungsverfahrensgesetzen etwa bestehendes Recht auf bloße Akteneinsicht. Schon angesichts des damit für den Verantwortlichen – hier: den Beitragsservice - verbundenen enormen zeitlichen, personellen und finanziellen Aufwands hätte ein solch umfassender Anspruch ausdrücklich in Art. 15 DSGVO normiert werden müssen. Darauf, dass dies ganz bewusst nicht geschehen ist, deutet nicht zuletzt Erwägungsgrund 63 DSGVO hin, nach dem es dem Verantwortlichen grundsätzlich möglich sein soll, vom Betroffenen präzise Angaben darüber verlangen zu können, auf welche Information oder welche Verarbeitungsvorgänge sich sein Auskunftsersuchen bezieht. Ein solches Korrektiv zur

[57] Zumindest innerhalb eines Arbeitsverhältnisses bejaht das LAG Baden-Württemberg, Urt. vom 20.12.2018 – 17 Sa 11/18 – einen Anspruch des Arbeitnehmers auf Kopie aller Unterlagen mit seinen personenbezogenen Daten

Vermeidung unverhältnismäßigen Aufwands wäre entbehrlich, wenn der Verantwortliche dem Betroffenen ohnehin sämtliche Einzeldaten in Kopie zur Verfügung zu stellen hätte.

158 Schließlich sprechen auch systematische Gründe gegen eine solch weitgehende Interpretation von Art. 15 Abs. 3 S. 1 DSGVO. So darf nach Art. 15 Abs. 4 DSGVO das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Wäre Abs. 3 S. 1 im Sinne eines Anspruchs auf Kopien sämtlicher Datenträger mit den personenbezogenen Daten des Betroffenen zu verstehen, müsste der Verantwortliche diese vor Aushändigung daraufhin überprüfen, ob dort enthaltene Angaben die Rechte und Freiheiten Dritter beeinträchtigen können. Es liegt auf der Hand, dass eine dahingehende Prüfung und entsprechende Bereinigung sämtlicher Datenträger gerade bei einem Massenaufkommen wie beim Beitragsservice kaum zu leisten und daher völlig unverhältnismäßig wäre. Darüber hinaus bliebe in diesem Falle auch für das in Art. 20 DSGVO konstituierte Recht auf Datenübertragbarkeit kein sinnvoller Anwendungsbereich mehr. Denn wenn der Betroffene schon nach Art. 15 Abs. 3 eine Kopie sämtlicher zu seiner Person verarbeiteten Einzeldaten verlangen kann, erschließt sich nicht, warum der Verantwortliche dann außerdem noch verpflichtet sein soll, ihm auf Verlangen diese Daten „in einem strukturierten, gängigen und maschinenlesbaren Format“ zur Verfügung zu stellen.

159 Dementsprechend habe ich die dazu bei mir eingegangenen Beschwerden als unbegründet zurückgewiesen. Zu einem Klageverfahren ist es daraufhin trotz vereinzelter Ankündigung bislang noch nicht gekommen. Angesichts der praktischen Konsequenzen im Falle einer weiten Auslegung dieser umstrittenen Vorschrift ist aber damit zu rechnen, dass die Frage über kurz oder lang höchstrichterlich (durch den EuGH) abschließend geklärt werden wird.

b Speicherung von Logdaten / SIEM

160 Intensiv hatte ich mich mit den Voraussetzungen für eine zulässige Speicherung der Logdaten über einen längeren Zeitraum für alle vom Verantwortlichen (gleich für welchen Zweck) eingesetzten Datenverarbeitungssysteme zu befassen. Anlass war die Bitte einer Rundfunkanstalt um eine förmliche Vorabkonsultation gemäß Art. 36 DSGVO im Zusammenhang mit einer vorsorglich durchgeführten Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO. Mir wurden dazu zahlreiche Unterlagen zur Verfügung gestellt, und ich habe das Vorhaben sowohl mit dem Datenschutz-, dem IT-Sicherheitsbeauftragten und Projektverantwortlichen als auch mit dem Vorstand der Personalvertretung der Rundfunkanstalt eingehend erörtert.

161 Ausgelöst wurde die Überlegung, den Zeitraum für die Speicherung aller Logdaten deutlich zu verlängern, durch die zunehmende Bedrohung der IT-Infrastrukturen durch Cyberattacken. Die automatisierte Speicherung von Logdaten für jedes eingesetzte Datenverarbeitungssystem ermöglicht es dem Verantwortlichen, nachträglich zu überprüfen und festzustellen, wer dort wann personenbezogene Daten eingegeben, gespeichert, verändert oder entfernt hat. Diese Kontrollfunktion ist ein geeignetes und sachlich gerechtfertigtes Mittel präventiven Datenschutzes und daher grundsätzlich zulässig, Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

162 Dabei ist eine längere Speicherdauer für sich genommen nicht geeignet, Attacken zu reduzieren oder sogar auszuschließen. Sehr wohl aber kann sie es mithilfe einer automatisierten Auswertung des Datenbestands ermöglichen, derartige Angriffe zu einem Zeitpunkt zu entdecken, in dem weitergehende, gravierendere Schäden noch verhindert und/oder Sicherheitsdefizite zumindest für die Zukunft beseitigt werden können. Innerhalb eines nur kurzen – hier bislang nur wenige Tage umfassenden - Zeitraums und ohne Gesamtbetrachtung aller vom Verantwortlichen eingesetzten Datenverarbeitungssysteme ist eine solche Kontrolle nicht vergleichbar wirksam möglich. Das BSI empfiehlt daher Betreibern Kritischer Infrastrukturen im Sinne des BSI-Gesetzes die Speicherung von Logdaten, jedenfalls für Proxy- und Firewall-Logs, für die Dauer von mindestens 90 Tagen.

163 Die Rundfunkanstalten selbst sind nicht als Betreiber einer solchen Kritischen Infrastruktur im Sinne des BSI-Gesetzes zu qualifizieren und unterliegen daher auch (noch) nicht dahingehenden Verpflichtungen (s.o. Rn. 35 ff.). Wohl aber ist der öffentlich-rechtliche Rundfunk nach der Rechtsprechung des Bundesverfassungsgerichts essentieller Bestandteil einer funktionsfähigen demokratischen Gesellschaft und hat infolge seiner spezifischen Konstruktion, Finanzierung und Aufgabe eine besondere Garantenstellung inne. Sein verfassungsrechtlicher Funktionsauftrag berechtigt und verpflichtet ihn gleichermaßen gegenüber der Allgemeinheit, deren Sachwalter er im Bereich des Rundfunks bzw. der elektronischen Massenkommunikation ist. Besonders bedeutsam für diesen Funktionsauftrag ist die Zuverlässigkeit vor allem seines Informationsangebots in doppelter Hinsicht (s. dazu bereits oben Rn. 86 ff.): Zum einen muss der öffentlich-rechtliche Rundfunk gewährleisten, dass seine Informationsangebote im Rahmen des technisch und wirtschaftlich Vertretbaren jederzeit der gesamten Bevölkerung frei zugänglich sind. Zum anderen muss sich die Bevölkerung auf die Authentizität und Integrität dieser Informationsangebote verlassen können. Diese Ausgangslage erfordert eine besondere Sensibilität der Rundfunkanstalten gegenüber einschlägigen Risiken. Dass die Rundfunkanstalten sich auf sie einstellen und ihnen mit besonderen Maßnahmen frühzeitig entgegenwirken, halte ich angesichts ihrer verfassungsrechtlichen Gewährleistungsverpflichtungen deshalb nicht nur für gerechtfertigt, sondern grundsätzlich sogar für geboten.

164 Es liegen hinreichend plausible Anhaltspunkte dafür vor, dass die Bedrohung durch Cyberattacken gerade auch im Bereich der elektronischen Massenmedien steigt. So hat etwa das Bundesamt für Verfassungsschutz anlässlich entsprechender Vorfälle unter anderem bei WDR und ZDF im Juli 2018 vor besonders „hochwertigen" Angriffen mit nachrichtendienstlichem Hintergrund auf deutsche Medienunternehmen gewarnt und eine längerfristige Logdatenspeicherung zumindest für Internet Proxy-Server empfohlen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betonte in seinem Lagebericht zur IT-Sicherheit 2018, dass Cyber-Sicherheit in der immer weiter fortschreitenden Digitalisierung kontinuierlich beachtet und dabei insbesondere die Sicherheitsarchitektur computergestützter Arbeitsplätze und Unternehmensabläufe von Anfang an die Gestaltung der IT-Infrastruktur einbezogen werden muss.

165 Die Belange der von der verlängerten Logdatenspeicherung betroffenen Personen (sowohl der Beschäftigten als auch Dritter) hatte die Rundfunkanstalt bei der Ausgestaltung aller vorgesehenen organisatorischen und technischen Maßnahmen grundsätzlich angemessen berücksichtigt. Vor diesem Hintergrund habe ich das Konzept für eine verlängerte Speicherung der Logdaten sowie die Auswertung der entsprechenden Daten im begründeten Fall des Verdachts auf einen Cyberangriff nach Maßgabe einiger zusätzlicher technischer und organisatorischer Vorkehrungen genehmigt.

166 Besser noch als das dort vorgesehene Verfahren ermöglicht der Einsatz eines sogenannten SIEM(Security Information and Event Management)-Tools im Zusammenspiel mit einem SOC (Security Operation Center) die Abwehr von Cyberattacken. Allerdings ist ein solches Instrument auch deutlich aufwändiger bzw. kostspieliger. Daher prüfen derzeit mehrere Rundfunkanstalten, ob sie eine solche Sicherheitseinrichtung gemeinsam einführen. Aus meiner Sicht wäre dies zu begrüßen, da die vielfältigen Verbindungen innerhalb des Systems des öffentlich-rechtlichen Rundfunks, jedenfalls aber im ARD-Verbund die Gefahr begründen, dass ein erfolgreicher Cyberangriff an einer Stelle sich rasch auf die Funktionsfähigkeit des Gesamtsystems auswirkt oder sich im System verbreitet. Die Integrität und Vertraulichkeit der Daten (Art. 5 Abs. 1 lit. f) DSGVO) ist daher nur so sicher gewährleistet wie beim schwächsten Glied der Kette (bzw. des Systems). Nicht nur deshalb haben entsprechende Vorhaben erkennbar strategische Bedeutung für den öffentlich-rechtlichen Rundfunk. Sie sollten daher gemeinschaftlich auf oberster Ebene und nicht ausschließlich am vordergründigen Maßstab des finanziellen Aufwands bewertet werden.

c Einsatz cloudbasierter Office-Systeme (Office 365)

167 Sogenannte Cloudanwendungen und -systeme ermöglichen es unter anderem, Datenbestände kostengünstig zu speichern und sie über das Internet ortsunabhängig – auch gemeinsam mit verteilten Nutzern – effizient und flexibel zu verarbeiten, ohne dafür selbst die entsprechenden Kapazitäten auf den jeweiligen Geräten oder im eigenen Unternehmen aufbauen und sichern zu müssen. Moderne Büroanwendungen wie etwa das Microsoft-Produkt „Office 365" nutzen ein solches Cloud-System als Basis ihres Funktionsangebots. Die damit verbundenen Vorteile wollen sich zunehmend auch die Rundfunkanstalten zunutze machen.

168 Jenseits der Frage, inwieweit sich die Rundfunkanstalten mit dem Einsatz derartiger Standardprodukte von einzelnen Software-Konzernen abhängig machen[58] Ob solche Systeme datenschutzkonform eingesetzt werden können, hängt allerdings von einer umfassenden Bewertung aller betroffenen Belange und Risiken, gegebenenfalls auch einer förmlichen Datenschutzfolgenabschätzung gemäß Art. 35 DSVGO ab. Vor allem soweit dabei die Dienste von Anbietern in Anspruch genommen werden sollen, die – wie bspw. Microsoft oder Amazon – ihren Sitz außerhalb der EU haben, besteht für die Verantwortlichen erheblicher Klärungs- und Regelungsbedarf, denn im Regelfall werden die Daten jeweils auf Servern außerhalb der EU verarbeitet. Zudem sind die Konzerne nicht oder nur eingeschränkt bereit, vertraglich die von der DSGVO geforderten Datenschutzstandards zu garantieren. Daher haben sich bereits mehrere staatliche Aufsichtsbehörden in unterschiedlicher Weise mit dem Thema beschäftigt – bis hin zum Verbot des Einsatzes von Office 365 in Schulen, das der Hessische Beauftragte für Datenschutz und Informationsfreiheit im Sommer 2019 zunächst verfügte, bis er die Anwendung unter Auflagen dann doch gestattete[59].

169 Auch im Falle der Rundfunkanstalten geht es vielfach um die Verarbeitung sensibler und daher besonders schutzwürdiger personenbezogener Daten – insbesondere natürlich im Bereich der journalistischen Tätigkeit. Vor diesem Hintergrund hat die RDSK ein von mir entworfenes Papier mit datenschutzrechtlichen Eckpunkten zum Einsatz cloudbasierter Office-Systeme verabschiedet, das den Verantwortlichen als Orientierungshilfe für die erforderliche Detailprüfung dienen soll[60]. Es fasst die

---

58 Siehe dazu in Bezug auf die Bundesbehörden die im Auftrag des Bundesministeriums des Innern, für Bau und Heimat (BMI) entstandene Marktanalyse von PwC vom August 2019, abrufbar unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.html?nn=4623908

59 Dazu bspw. TB des Beauftragten für Datenschutz und Informationsfreiheit des Landes Rheinland-Pfalz, S. 99 ff.; https://www.datenschutz.rlp.de/fileadmin/lfdi/Taetigkeitsberichte/ds_tb26.pdf

60 https://www.rundfunkdatenschutz.de/infothek/einsatz-cloudbasierter-office-systeme-.file.html/Cloudbasierte%20Office-Systeme_2020-02-10.pdf

wichtigsten dabei zu klärenden Aspekte zusammen und skizziert die zu berücksichtigenden organisatorischen, personellen und technischen Maßnahmen. Insbesondere müssen die Verantwortlichen

- die in der Cloud zu verarbeitenden personenbezogenen Daten mit Blick auf ihren Schutzbedarf klassifizieren und darauf bezogen die Autorisierungs- und Authentifikations-Vorgaben bzw. -Maßnahmen festlegen. Auch in Bezug auf private Nutzung und den dienstlichen Einsatz privater Geräte müssen die Rechte der Betroffenen abgewogen werden.
- verbindliche Nutzervorgaben entwickeln und die Zielgruppen sensibilisieren,
- je nach eingesetztem Produkt technische Datenzugriffs- und –sicherungsvorkehrungen vorsehen. So müssen grundsätzlich nicht benötigte Funktionen deaktiviert und dürfen nur die notwendigen Funktionen freigeschaltet sein. Dem Schutz vor unberechtigtem Zugriff dienen Verschlüsselungsmechanismen und detaillierte Vorgaben zur Schlüsselverwaltung.

d Nutzung von „Social Media“

170 Ein Thema, das mich vielfach und in unterschiedlicher Weise beschäftigt hat, ist die Nutzung sogenannter Social Media-Dienste in den Programmen der Rundfunkanstalten. Insbesondere äußern immer wieder Hörer bzw. Zuschauer ihr Unverständnis oder beschweren sich darüber, dass der öffentlich-rechtliche Rundfunk solche Plattformen bedient, die sie als ausländische „Datenkraken“ wahrnehmen.

171 Typischerweise und grob zu unterscheiden sind dabei jedenfalls die folgenden Konstellationen:

- Die Rundfunkanstalt nutzt Social Media als Verbreitungsplattform für ihre Angebote, um dort neues bzw. zusätzliches Publikum zu erreichen. Ob und inwieweit dies statthaft ist, entscheidet sich primär nach rundfunk- (programm-) und lizenzrechtlichen Maßgaben. Datenschutzfragen sind davon nicht unmittelbar berührt.
- Die Rundfunkanstalt weist in ihren Programmen auf Angebote bestimmter Social Media-Plattformen hin. Auch hier geht es in erster Linie, etwa mit Blick auf das Gebot der Trennung von Werbung und Programm, um Fragen der Programmgestaltung. Datenschutzfragen sind davon allenfalls in allgemeiner Form berührt.
- Die Rundfunkanstalt fordert Hörer bzw. Zuschauer dazu auf, die von ihr gestaltete Präsenz auf einer bestimmten Social Media-Plattform zu besuchen bzw. nutzen. Neben Aspekten des Rundfunk- bzw. Programmrechts geht es insoweit auch um Datenschutzaspekte.
- Und schließlich setzt die Rundfunkanstalt eine Social Media-Plattform als Programmelement im Sinne eines Interaktionsinstruments sein. Dies wirft neben etwaigen rundfunk- vor allem datenschutzrechtliche Fragen auf.

172 Die für eine aktive Nutzung solcher Drittplattformen ins Feld geführten Gründe (insbesondere die Ansprache vor allem jüngerer Zielgruppen, zusätzliche Kommunikations- und Interaktionsoptionen etc.) habe ich in datenschutzrechtlicher Hinsicht nicht zu bewerten. Zu berücksichtigen ist zudem, dass im Bereich der Datenverarbeitung zu journalistischen Zwecken die datenschutzrechtlichen Vorgaben nur eingeschränkt gelten („Medienprivileg", s.o. Rn. 8 ff.). Soweit die Rundfunkanstalten also Drittplattformen nutzen, um ihr publizistisches Angebot zu erweitern bzw. zu verbreiten, sind sie beispielsweise nicht an die Regelungen zur gemeinsamen Verantwortung (Art. 26 DSGVO) oder zur Auftragsverarbeitung (Art. 28 DSGVO) gebunden. Dabei kann im Einzelfall unter anderem relevant sein, ob und inwieweit es sich tatsächlich um eine Datenverarbeitung zu journalistischen Zwecken handelt; für die Nutzung als „Ausspielweg" für journalistische Inhalte jeder Art allerdings ist diese Zielsetzung unzweifelhaft.

173 Deshalb sind diese Aktivitäten unter der Datenschutzperspektive allerdings für mich nicht irrelevant. Denn auch wenn und soweit für ihn die gesetzlichen Freiräume des „Medienprivilegs" greifen sollten, unterliegt der öffentlich-rechtliche Rundfunk nach meinem Verständnis dabei doch besonderen Fürsorge- und Aufklärungsobliegenheiten. Mit seinen Aktivitäten veranlasst er sein Publikum dazu, Drittplattformen zu nutzen, die die Standards des europäischen und deutschen Datenschutzrechts nicht annähernd einhalten[61]; er trägt insoweit daher eine gewisse Mitverantwortung für das Verhalten der Nutzer, an die er sich aktiv wendet. Ein solches Rollenverständnis sollte ihn deshalb zu einer besonders umfassenden, verständlichen, zielgruppenspezifischen Information und Aufklärung seines – insbesondere jüngeren - Publikums über die damit verbundenen Folgen für die Verarbeitung der Nutzerdaten veranlassen.

174 Dafür sollten die Rundfunkanstalten sämtliche ihnen zu Gebote stehenden publizistischen Mittel einsetzen, also nicht nur besonders verständliche und handhabbare Datenschutzhinweise bzw. -erklärungen im eigenen Onlineangebot, sondern auch zielgruppenspezifische audiovisuelle Beiträge im Programm. In zahlreichen Sendungen befassen sich die Rundfunkanstalten auch immer wieder mit Datenschutzthemen – überwiegend allerdings jeweils aus aktuellem Anlass und nicht systematisch. Immerhin sind die entsprechenden Beiträge regelmäßig für einige Zeit in den Mediatheken abrufbar. Auf diese Option mache ich deshalb auch auf meiner Homepage ausdrücklich aufmerksam[62].

---

61 Besonders problematisch ist insoweit das chinesische Angebot „TikTok", das sich gezielt an Kinder und Jugendliche richtet. Nach seiner Datenschutzerklärung verarbeitet es sämtliche Kontakt– und technischen Daten der Nutzer und der von ihnen eingesetzten Geräte, IP-Adresse, Browserverlauf, Mobilfunkanbieter, Nutzungs- und Inhaltsdaten, Kommunikationspräferenzen und -daten sowie Daten anderer sozialer Netzwerke oder öffentlicher Foren (Profile, Freundeslisten, Login-Daten).

62 https://www.rundfunkdatenschutz.de/infothek/

175 Darüber hinaus könnten die Rundfunkanstalten ihre publizistischen Kapazitäten idealerweise aber auch dazu nutzen, einzelne Themen wie auch Elemente ihrer Datenschutzerklärungen in medial aufbereiteter, sowohl medien- wie auch zielgruppenspezifischer Form verständlich zu erläutern. Dies drängt sich vor allem für das ARD-/ZDF-Jugendangebot „funk" auf, das hauptsächlich auf die Nutzung von Drittplattformen setzt. Daher möchte ich mich in den kommenden Jahren verstärkt dafür einsetzen, dass der öffentlich-rechtliche Rundfunk seine Verantwortung annimmt und sein für eine medienspezifische Information und Aufklärung vorhandenes Potential ausschöpft.

e Platzierung, Gestaltung und Formulierung von Datenschutzhinweisen

176 Die Bevölkerung richtet besondere Erwartungen an das Verhalten des öffentlich-rechtlichen Rundfunks. Zurecht: Eine Einrichtung, die die Allgemeinheit finanziert und der sich daher niemand „entziehen" kann, sollte sich besondere Mühe damit geben, ihr Handeln verständlich zu erklären. Das gilt auch und gerade in Bezug auf Datenschutzthemen.

177 In diesen Kontext sind mehrere bei mir eingegangene Zuschriften zur Formulierung, Gestaltung und Platzierung von Datenschutzerklärungen bzw. Cookie-Hinweisen einzuordnen. Die Beschwerdeführer monierten unter anderem nicht ausreichend konkrete Erläuterungen zum Einsatz und zur Wirkungsweise von Cookies und Apps, zur Berechtigung der Datenverarbeitung für Zwecke der Nutzungsmessung (dazu auch unten Rn. 183 ff.) sowie zur Einbindung von Drittplattformen oder von sonstigen Dritten, etwa im Bereich der Auftragsproduktion für bestimmte Fernsehformate oder Gewinnspiele. Außerdem ging es um die Verständlichkeit und Nachvollziehbarkeit bestimmter Erläuterungen, insbesondere in Bezug auf Angebote, die sich (auch) an Kinder und Jugendliche richteten, und die Zulässigkeit einer Weiterverweisung in Bezug auf die Datenschutzhinweise in einer App per Link auf die Datenschutzerklärung der Homepage (sog. „Medienbruch").

178 Der rechtliche Maßstab für die Inhalte der Datenschutzerklärungen ergibt sich aus den Vorschriften des Art. 13 DSGVO. Nach allgemeiner Auffassung wird der Verantwortliche seiner Informationspflicht nur dann gerecht, wenn die entsprechenden Erläuterungen verständlich und leicht zugänglich sind. In diesem Zusammenhang ist auch die oben angesprochene Frage des „Medienbruchs" bedeutsam: Leicht zugänglich ist die Datenschutzerklärung nach Auffassung der europäischen Datenschutzaufsichten[63] nur, wenn der Nutzer auf den ersten Blick erkennen kann, wo die Informationen zum Datenschutz abrufbar bzw. zugänglich sind. Eine Möglichkeit, diese Anforderungen (auch in einer App) zu erfüllen, ist es, dass die Infor-

[63] Siehe Working Paper No. 260 Rn. 11 der vormaligen „Art. 29-Gruppe", https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

mationen „nie mehr als zwei Schritte entfernt“ sind. „Datenschutz“ sollte deshalb stets als eigener Menüpunkt vorgesehen werden, und die Datenschutzerklärung muss entweder im Angebot (also auch einer App) selbst oder über einen Link unmittelbar bzw. leicht erreichbar sein.

179 Sowohl in diesem wie auch in den anderen monierten Punkten genügten die entsprechenden Erklärungen bzw. Hinweise der Rundfunkanstalten nach meiner Prüfung letztlich den gesetzlichen Anforderungen. Gleichwohl hätte die eine oder andere Formulierung präziser oder verständlicher formuliert sein können. Meine dahingehenden Hinweise bzw. Empfehlungen sind durchweg befolgt bzw. umgesetzt worden.

180 Dass auch ansonsten bei genauerer Betrachtung öffentlich-rechtlicher Onlinepräsenzen durchaus noch einiger Optimierungsanlass feststellbar ist, hat zumindest in Bezug auf die Datenschutzhinweise bei ard.de bzw. Das Erste.de auch die im Auftrag des Bundesministeriums für Justiz und Verbraucherschutz entstandene Studie zur Umsetzung der Anforderungen der DSGVO durch Online-Portale gezeigt (s.o Rn. 74). Ich werde mich weiter dafür einsetzen, dass sich der öffentlich-rechtliche Rundfunk hierbei durchaus in einer Vorbildrolle sieht und sich nicht nur damit begnügt, allenfalls gesetzliche Mindeststandards einzuhalten (geschweige denn, hinter ihnen zurückzubleiben).

f Verarbeitung von Nutzungsdaten

181 Immer wieder zeigen sich Petenten irritiert darüber, dass „ausgerechnet der öffentlich-rechtliche Rundfunk“ ihre Nutzungsdaten ohne ihre Kenntnis bzw. Einwilligung auswertet – erst recht, wenn und soweit es dabei um Angebote geht, die sich an Kinder und Jugendliche richten.

182 Damit ist eines der praktisch bedeutsamsten, strittigsten und deshalb auch vielfach in den Medien aufgegriffenen Datenschutz-Themen überhaupt angesprochen: das Erheben und Verarbeiten von Nutzerdaten, auch über einzelne Onlineangebote hinweg (Tracking). Üblicherweise wollen Telemedienanbieter damit die Möglichkeit erhalten, Nutzerprofile für zielgenau platzierbare Werbung und auf diese Weise höhere Einnahmen zu generieren. Technisch ermöglicht wird eine solche Datenverarbeitung durch kleine Textdateien, die auf dem Gerät des Nutzers zu den besuchten Webseiten gespeichert werden und den Webserver damit in die Lage versetzen, bei jedem folgenden Besuch die jeweils erfassten Daten (wie etwa die sogenannte Session ID, Login-Daten, Angaben zum Warenkorb eines Bestellvorgangs u.a.m.) zu nutzen. Diese Dateien werden mit dem Oberbegriff „Cookies“ bezeichnet.

183 Während es dabei also typischerweise um rein wirtschaftliche Interessen geht, dient die Nutzungsmessung den Rundfunkanstalten ausschließlich zu publizistischen Zwecken, nämlich dazu, ihre Angebote redaktionell optimal aufzubereiten und zu präsentieren und damit eine möglichst große Nachfrage und Resonanz zu erzielen. Insoweit beschwerten sich Beschwerdeführer bei mir etwa darüber, dass ihre Nutzungsdaten ausgewertet wurden, obwohl sie dem nicht zugestimmt (kein „Opt-In") oder sogar ausdrücklich widersprochen („Opt-Out") hätten. Sie problematisierten außerdem, dass aus den Daten womöglich politische oder sonstige inhaltliche Präferenzen der Onlinenutzer ableitbar seien. Und es sei nicht nachvollziehbar, warum die Rundfunkanstalten für die Nutzungsmessung unterschiedliche externe Dienstleister einsetzten, zumal diese womöglich ihrerseits die erhobenen Daten für eigene bzw. sonstige (geschäftliche) Zwecke weiternutzten; dies lege zumindest deren eigene Datenschutzerklärung nahe.

184 Im Ergebnis haben meine Prüfungen in keinem der entsprechenden Fälle Anhaltspunkte für einen Verstoß der Rundfunkanstalten gegen Datenschutzvorschriften ergeben, wohl aber aufgezeigt, dass diese hier in einem sensiblen Bereich tätig sind. Da im allgemeinen gerade Cookies, die das Nutzungsverhalten erfassen und auswerten, nur mit ausdrücklicher Einwilligung der betroffenen Person eingesetzt werden dürfen, entsteht erhöhter Aufklärungs- und Beratungsbedarf, wenn und soweit die Rundfunkanstalten keine Einwilligung einholen. Auf eine solche dürfen sie in Bezug auf die Nutzungsmessung in der Tat verzichten, weil diese ihrem verfassungsrechtlichen Funktionsauftrag dient, auf dessen Grundlage sie die Bevölkerung auf allen für elektronische Medien relevanten Märkten mit einem publizistisch konkurrenzfähigen Angebot zu versorgen haben. Daher können sich die Rundfunkanstalten hier auf Art. 6 Abs. 1 S. 1 lit. e) (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) und lit. f) (Wahrung berechtigter Interessen) DSGVO stützen. Zu berücksichtigen ist außerdem, dass sie dafür ausschließlich anonymisierte bzw. pseudonymisierte Daten auswerten (lassen), sodass sie schon technisch nicht in der Lage sind, personenbezogene Nutzungsprofile anzulegen und auszuwerten.

185 Dies gilt auch, soweit die Rundfunkanstalten auf unterschiedliche Dienstleister zurückgreifen, die jeweils die Nutzung spezifischer Teilelemente des Onlineangebots auswerten (beispielsweise die Akzeptanz von Streaming-Angeboten, den Nutzungsanteil von Videos oder Audios, die Nachfrage nach bestimmten Themen, Messung von Page-Impressions und Visits u.a.m.). Alle Dienstleister sind im Rahmen von Auftragsverarbeitungsverhältnissen vertraglich verpflichtet, die Datenschutzvorgaben der Rundfunkanstalten einzuhalten, und unterliegen insoweit auch der Aufsicht des Rundfunkdatenschutzbeauftragten.

186 Dass die Rundfunkanstalten den Nutzern die Gelegenheit geben, der Nutzungsmessung zu widersprechen („Opt-Out"), ist datenschutzrechtlich gleichwohl zu begrü-

ßen. Allerdings sind inzwischen mehrere Browseranbieter dazu übergegangen, den Einsatz sogenannter Third-Party-Cookies automatisch zu unterbinden, mit der Folge, dass eine auf einem entsprechenden Cookie basierende Datenverarbeitung nicht mehr funktioniert.

187 Insgesamt zeigen die bei mir eingehenden Anfragen und Beschwerden, dass die Rundfunkanstalten ihre Datenschutzerklärungen bzw. Cookie-Hinweise zu diesem sensiblen Themenfeld besonders sorgfältig und verständlich formulieren sollten (s. bereits oben Rn. 178 ff.). Allgemeinplätze wie etwa das Bestreben, mithilfe eines Cookies „den Nutzern ein bestmögliches Angebot zur Verfügung zu stellen", werden dem nicht gerecht. Wichtig ist es insbesondere, die spezifische Aufgabe und Funktion des öffentlich-rechtlichen Rundfunks zu erläutern und die sich daraus ergebende Rechtsgrundlage für den Einsatz der betreffenden Cookies zu nennen.

g Personalisierungsfunktionen

188 Auch die Frage, ob und unter welchen Voraussetzungen es zulässig ist, die personalisierte Nutzung der öffentlich-rechtlichen Onlineangebote – insbesondere der ZDF-Mediathek - zu ermöglichen, hat mich mehrfach beschäftigt. So wurde etwa beanstandet, dass die für die Einrichtung eines solchen Accounts notwendige Einwilligung sich nicht zugleich auf die Bereitschaft etwa zu persönlichen Empfehlungen oder Personalisierungen erstrecken dürfe, da sie unter dieser Voraussetzung nicht als „freiwillig" zu bezeichnen sei. Außerdem sei es unzulässig, für die Altersverifikation Personalausweisdaten anzufordern und zu verarbeiten.

189 Im Ergebnis meiner Prüfung habe ich jedoch auch hier keinen Verstoß gegen datenschutzrechtgliche Vorgaben erkennen können. Tatsächlich macht das ZDF die Einrichtung eines personalisierten Accounts davon abhängig, dass sich die Person, die die mit diesem Angebot verbundenen Möglichkeiten nutzen möchte, damit einverstanden erklärt, dass das ZDF die Daten für "persönliche Empfehlungen" verarbeitet. Das dafür vorgesehene Kästchen ist zwar nicht vorab angekreuzt, aber ohne Ankreuzen ist eine Registrierung nicht möglich. Erst nach einer solchen Registrierung hat die betreffende Person die Möglichkeit, die Empfehlungsfunktion abzustellen. Dennoch ist die Einwilligung als „freiwillig" im Sinne von Art. 4 Nr. 11 DSGVO zu qualifizieren, und zwar auch nach den Maßstäben, die der EuGH in seinem Urteil vom 1. Oktober 2019 (s.o. Rn. 55 ff.) entwickelt hat.

190 Für die insoweit anzustellende Gesamtbetrachtung ist unter anderem maßgeblich, dass die Einwilligung nicht etwa für die Nutzung der Mediathek als solche, sondern lediglich für deren personalisierte Ausgestaltung bzw. Nutzung erforderlich ist. Dafür werden bestimmte Funktionalitäten gebündelt zur Verfügung gestellt, etwa die Möglichkeit, bereits begonnene Videos zu einem späteren Zeitpunkt ab der zuletzt

betrachteten Sequenz weiterzuschauen, jugendschutzrelevante Beiträge auch außerhalb der für das Fernsehprogramm geltenden Tageszeiten zu sehen, eine persönliche Merkliste anzulegen, Sendungen zu abonnieren oder Empfehlungen zu erhalten. In rechtlicher Hinsicht wird den Nutzern diese Funktion auf der Basis eines Vertrags angeboten, den sie durch ihre Registrierung zunächst nur insgesamt annehmen können. Allerdings haben sie nach Abschluss des Vertrags sehr wohl die Möglichkeit, einzelne der davon umfassten Funktionen auszuschließen oder aber den Vertrag insgesamt rückgängig zu machen. Weitere Nachteile als die mit der entsprechenden Erklärung unmittelbar verbundenen (und im Falle des „Opt-Out" auch beabsichtigten) Folgen sind damit nicht verbunden.

191 Dass der öffentlich-rechtliche Rundfunk aus dem Rundfunkbeitrag und damit von der Allgemeinheit finanziert wird, verpflichtet ihn nicht, jedem Onlinenutzer ein personalisiertes Angebot zu jeweils individuellen Bedingungen bzw. jeweils spezifischen Vertragskonditionen zur Verfügung zu stellen. Abgesehen davon, dass eine vollständig personalisierte Nutzung mit einem enormen finanziellen Aufwand (und damit auch einem erhöhten Rundfunkbeitrag) verbunden wäre, ließe sich dies wiederum auch nur mit einer Personalisierungsfunktion für sämtliche Nutzer der Mediathek sowie deren laufender Überprüfung bzw. Aktualisierung umsetzen. Gerade aus datenschutzrechtlicher Sicht wäre der Aufbau einer derart umfassenden Datenbank jedoch die deutlich problematischere Variante.

192 Was die Frage der Altersverifikation betrifft, folgt bereits aus den ihm obliegenden allgemeinen Sorgfaltspflichten, dass der öffentlich-rechtlichen Rundfunk die für ihn maßgeblichen jugendschutzrechtlichen Sendezeitrestriktionen auch zu beachten hat, soweit er seine Beiträge online verfügbar macht; im übrigen schreiben dies die Vorschriften des Jugendmedienstaatsvertrags auch ausdrücklich vor. Dass sich Kinder und Jugendliche im Internet heutzutage jederzeit anderweitig Zugang zu zahllosen insoweit problematischen Inhalten verschaffen können, rechtfertigt es nicht, den öffentlich-rechtlichen Rundfunk von diesen Bindungen zu befreien. Wenn die Rundfunkanstalten also für die Freigabe von Sendungen jenseits der jugendmedienschutzrechtlich gebotenen Sendezeitvorgaben die Angabe von Teilen der Personalausweisnummer verlangen, ist dies ein geeignetes und datenschutzrechtlich zulässiges Mittel, wenn und soweit sie diese Daten lediglich für einen einmaligen automatisierten Abgleich nutzen und nicht speichern oder anderweitig verarbeiten. Diese Voraussetzung ist in den hier in Rede stehenden Fällen jeweils erfüllt.

h HbbTV: IP-Autostart

193 Zunehmend lösen sogenannte Smart-TV-Geräte den klassischen Fernseher ab. Der wesentliche Unterschied besteht darin, dass die neuen Geräte nicht nur das klassische Funk- (terrestrisch oder Satellit) oder Kabelsignal empfangen, sondern auch

über einen Internetanschluss verfügen und so die Nutzung von HbbTV(Hybrid Broadcast Broadband TV)-Programmen mit ihren zahlreichen Zusatzangeboten ermöglichen. Diese Optionen kann der Nutzer über den „Red Button" auf der Fernbedienung an- und auswählen. Dafür wird bereits bei Aufruf eines Senders mittels einer über das Rundfunksignal versandten URL automatisch eine Internet-Verbindung zum Server des HbbTV-Anbieters hergestellt, um die Zusatzinformationen schon vor dem Drücken des Red-Buttons auf der Fernbedienung im Hintergrund zu laden. Dies vermeidet längere Wartezeiten nach dem Drücken des Red Button und ist im HbbTV-Standard technisch so vorgegeben.

194 In datenschutzrechtlicher Hinsicht stellt sich insoweit allerdings die Frage, ob und auf welcher Grundlage die IP-Adresse – bei der es sich nach der Rechtsprechung des EuGH um ein personenbezogenes Datum handelt - zulässigerweise an die HbbTV-Anbieter übermittelt wird. Mit ihr hat sich die RDSK eingehend beschäftigt und dazu im Dezember ein Positionspapier veröffentlicht[64]. Da die Nutzung von HbbTV vom verfassungsrechtlichen Funktionsauftrag des öffentlich-rechtlichen Rundfunks umfasst ist, können sich die Rundfunkanstalten insoweit auf Art. 6 Abs. 1 lit. e), außerdem aber – ebenso wie die anderen Rundfunkveranstalter - auch auf Art. 6 Abs. 1 lit. f) DSGVO stützen. Dies gilt allerdings ausschließlich, soweit das Signal dazu dient, um die Übertragung der HbbTV-Zusatzangebote zu ermöglichen; eine weitere Verarbeitung, insbesondere Speicherung oder Verknüpfung der Daten etwa mit dem Ziel, ein Nutzerprofil zu generieren, wäre ohne Einwilligung der betroffenen Person oder eine ausdrückliche gesetzliche Grundlage unzulässig.

i Datenschutz und Datenschutzaufsicht im journalistischen Bereich

195 Anfragen und Beschwerden unterschiedlichster Art haben mich zu Themen mit unmittelbarem oder mittelbarem Programmbezug erreicht. Grundsätzlich sind insoweit die bereits geschilderten Besonderheiten in materiell- und aufsichtsrechtlicher Hinsicht maßgeblich (s.o. Rn. 8 ff.). In der Regel habe ich die Petenten deshalb wegen der von ihnen behaupteten Persönlichkeitsrechtsverletzungen an die jeweils verantwortliche Rundfunkanstalt verwiesen. Auch Ersuchen auf Auskunft über die einem Beitrag zugrunde liegenden Unterlagen (§ 9c Abs. 3 RStV) waren zunächst an die Verantwortlichen und nicht an mich als Aufsichtsbehörde zu richten.

196 In einigen Fällen waren allerdings durchaus grundsätzlichere Aspekte berührt. So stellen sich im Bereich der **Auftragsproduktionen** im Binnenverhältnis zwischen der Rundfunkanstalt und dem Produktionsunternehmen Fragen der datenschutzrechtlichen Vertragsgestaltung (und damit verbunden der aufsichtsrechtlichen Zuständigkeit), weil zu den Regelungen, die im journalistischen Bereich nicht unmit-

64 https://www.rundfunkdatenschutz.de/infothek/hbbtv-ip-autostart.file.html/HbbTV_IP%20Autostart%2020191218.pdf

telbar gelten, nach § 9c RStV auch die zur gemeinsamen Verantwortung (Art. 26 DSGVO) bzw. Auftragsverarbeitung (Art. 28 DSGVO) gehören. Auch im Außenverhältnis (zu den Onlinenutzern) kann dies datenschutzrechtlich relevant werden, wenn und soweit beispielsweise bestimmte Seiten einzelner Sendeformate auf die Homepage der Auftragsproduzenten verlinken. In solchen Fällen sollte die Rundfunkanstalt ihre Nutzer jedenfalls dann hinreichend deutlich über die datenschutzrechtliche Verantwortlichkeit informieren, wenn sie sie auf diesem Weg zur Mitwirkung und damit verbunden zur Übermittlung ihrer personenbezogenen Daten (an den Auftragnehmer) veranlassen möchte.

197 Zu befassen hatte ich mich außerdem mit den Anforderungen an eine **Akkreditierung** von Beschäftigten der Rundfunkanstalten für die Berichterstattung von Spielstätten der Fußball-Bundesliga und der Nationalmannschaft. Zu den Daten, von deren Mitteilung die DFL die Akkreditierung abhängig machte und deren Übermittlung sie innerhalb einer regelmäßig äußerst kurzen Frist von 24 Stunden forderte, gehörte unter anderem das Geburtsdatum sowie der Wohnort der betreffenden Personen, unabhängig von ihrer jeweiligen Beschäftigung (Redaktion, Produktion, Technik etc.). Über alle Rundfunkanstalten hinweg betraf dies weit mehr als 100 Personen. Zur Begründung verwies die DFL lediglich allgemein auf potentielle Sicherheitsrisiken und die Notwendigkeit kurzfristiger „Zuverlässigkeitsüberprüfungen" des Personals[65].

198 Nach gemeinsamer Auffassung aller mit diesem Vorgang befassten Mitglieder der RDSK konnte diese pauschale Begründung die mit der Abfrage verbundene Vorratsdatenspeicherung der beiden sensiblen personenbezogenen Daten nicht rechtfertigen. Dies galt umso mehr, als die dazu befragten Sicherheitsbehörden mitteilten, dass sie selbst die Angabe dieser Daten für ihre Zwecke nicht benötigten. Diese ihre Rechtsauffassung konnten die Mitglieder der RDSK allerdings gegenüber der DFL GmbH nicht unmittelbar durchsetzen, da für die Datenschutzaufsicht dieses Unternehmens mit Sitz in Frankfurt/Main der Hessische Beauftragte für Datenschutz und Informationsfreiheit zuständig ist. Zudem zog sich die Klärung des Sachverhalts deshalb in die Länge, weil außer der DFL GmbH an dem Vorgang auch deren Produktionsgesellschaft Sportcast GmbH mit Sitz in Köln beteiligt war, sodass zudem auch noch die aufsichtsrechtliche Zuständigkeit zwischen Hessen und Nordrhein-Westfalen abzustimmen war.

199 Schlussendlich veranlasste der Hessische Beauftragte für Datenschutz und Informationsfreiheit die DFL GmbH jedoch, ihre Akkreditierungspraxis zu ändern, auf die Forderung nach Übermittlung von Geburtsdaten und privater Anschrift des Rund-

[65] Zu den nach ihrer Auffassung insoweit maßgeblichen datenschutzrechtlichen Grundsätzen siehe die Entschließung der DSK vom 26.4.2018, https://www.datenschutzkonferenz-online.de/media/en/20180426_en_zuverlaessigkeitspruefungen_veranstaltungen.pdf

funkpersonals künftig zu verzichten und die bis dahin erhobenen entsprechenden Daten zu löschen.

200 Staatliche und Rundfunkdatenschutzaufsicht gleichermaßen sind auch betroffen, wenn es um **Dreharbeiten bei Polizeieinsätzen** geht. Typischerweise gilt für alle unmittelbar programmbezogenen – journalistischen – Aktivitäten das Medienprivileg, und in Zweifelsfällen ist die Rundfunkdatenschutzaufsicht zuständig. Soweit es allerdings um die Bereitschaft der Polizei geht, sich bei der Arbeit begleiten zu lassen, sind für die Klärung etwaiger datenschutzrechtlicher Fragen deren behördliche Datenschutzbeauftragte sowie die jeweilige staatliche Datenschutzaufsichtsbehörde zuständig. Daraus folgt allerdings nicht etwa, dass die staatliche Aufsicht womöglich Vorgaben zur Gestaltung oder Ausstrahlung eines entsprechenden Programmbeitrags bzw. zur Verarbeitung, insbesondere Speicherung der dabei verarbeiteten personenbezogenen Daten machen könnte. Die Entscheidung darüber liegt vielmehr weder bei der Rundfunk- noch gar bei der staatlichen Datenschutzaufsicht, sondern ausschließlich in der Verantwortung der Rundfunkanstalt.

201 Schließlich sei als interessanter Fall aus dem Bereich der Datenverarbeitung für journalistische Zwecke noch die als „**Ibiza-Video**“ berühmt gewordene Veröffentlichung heimlich entstandener Aufnahmen des vormaligen FPÖ-Vorsitzenden Strache und weiterer Personen erwähnt. Mit ihr war ich in meiner Aufsichtspraxis zwar nicht unmittelbar befasst, aber das Thema vermittelte doch einen Eindruck von der Reichweite und vor allem vom Verständnis des sogenannten „Medienprivilegs“. Denn aus den Reihen der staatlichen Datenschutzaufsichten war die Auffassung zu vernehmen, die Süddeutsche Zeitung bzw. der SPIEGEL habe mit der Veröffentlichung des Videos die Grenzen des datenschutzrechtlich Zulässigen deshalb überschritten, weil es völlig ausreichend gewesen wäre, den wesentlichen Inhalt der Aufnahme in schriftlicher (und damit pressetypischer) Form zu veröffentlichen. Diese Bewertung allerdings verkennt völlig die Bedeutung, die einer Darstellung in Ton und Bild gerade in einem politisch und gesellschaftlich derart bedeutsamen Kontext wie in diesem Fall zukommt. Nach meiner Überzeugung war die Veröffentlichung des Videos unabhängig davon gerechtfertigt, dass Presseverlage generell berechtigt sind, Bewegtbildaufnahmen in ihren Onlineangeboten zu veröffentlichen, und insoweit nicht mehr nur herkömmlich mit Schrift und Bild agieren. In jedem Falle ist die Entscheidung darüber, ob vorhandenes Ton- und/oder Filmmaterial - in gegebenenfalls journalistisch bearbeiteter Form – vollständig oder nur als Abschrift oder gar nur schriftlich zusammengefasst veröffentlicht wird, vom „Medienprivileg“ umfasst und daher nicht datenschutzrechtlich determiniert. Entsprechendes gilt für die Bewertung der Frage, ob die betreffenden Aufnahmen rechtmäßig zustande gekommen sind.

j Beschäftigtendatenschutz

202 Mit Fragen zum Beschäftigtendatenschutz haben mich ausschließlich im Rahmen einer Erörterung mit den Verantwortlichen bzw. ihren Datenschutzbeauftragten in meinem Zuständigkeitsbereich befasst. Beschwerden dazu sind nicht eingegangen. Das spricht zunächst einmal dafür, dass der Schutz der personenbezogenen Daten aller Beschäftigten bei den damit befassten Stellen einerseits sowie den internen Datenschutzbeauftragten andererseits in besten Händen ist.

203 In unterschiedlichen Zusammenhängen hat die datenschutzrechtliche Einordnung der Mitarbeitervertretungen eine Rolle gespielt. Insoweit ging es einerseits um die Frage, ob der **Personal- oder Betriebsrat als Verantwortlicher** im Sinne des Art. 4 Nr. 7 DSGVO zu qualifizieren ist. Das ist nach meiner Auffassung nicht der Fall. Denn die Beschäftigtenvertretung ist keine Stelle, die (wie eine natürliche oder juristische Person, Behörde oder sonstige Einrichtung) allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Denn sie nimmt ihre Aufgaben zwar völlig eigenständig und unabhängig wahr, aber ausschließlich nach Maßgabe des jeweils einschlägigen Personalvertretungsrechts und deshalb nicht nach freier eigener Entscheidung. Dabei greift sie in vollem Umfang auf die technische und sonstige Infrastruktur des Betriebs zurück. Wäre die Mitarbeitervertretung dennoch als datenschutzrechtlich „Verantwortlicher“ zu qualifizieren, müsste nicht nur der jeweilige Verantwortungsbereich voneinander abgegrenzt und eine etwaige gemeinsame Verantwortung definiert werden, sondern sie wäre grundsätzlich auch verpflichtet, eine eigene interne Datenschutzbeauftragte zu benennen. Zudem trüge sie das volle Haftungsrisiko für sämtliche Datenschutzverstöße in ihrem Bereich – allerdings ohne das damit sonst verbundene wirtschaftliche Risiko, da die finanziellen Konsequenzen letztlich doch das Unternehmen zu tragen hätte.

204 Daraus folgt nach meiner Auffassung außerdem die **Zuständigkeit der internen Datenschutzbeauftragten** der Rundfunkanstalt bzw. des Unternehmens jeweils auch für die Überwachung und Beratung des Datenschutzes in den Mitarbeitervertretungen (s. auch unten Rn. 211 ff.). Dies hat das Bundesarbeitsgericht im Jahr 1998 in Bezug auf den Betriebsrat noch anders beurteilt[66]. Denn in der Regel bestelle die verantwortliche Stelle den Datenschutzbeauftragten allein bzw. einseitig, sodass dieser im Verhältnis zur Mitarbeitervertretung, deren Rolle typischerweise die des Gegenparts zur Geschäftsleitung sei, als „verlängerter Arm“ des Arbeitgebers wahrgenommen werden könne. Ein Kontrollrecht des Datenschutzbeauftragten sei daher mit der vom Betriebsverfassungsgesetz (BetrVG) vorgeschriebenen Unabhängigkeit des (Gesamt-)Betriebsrats vom Arbeitgeber unvereinbar.

66 BAG, B. v. 11.11.1998 – 1 ABR 21/97 -, NZA 1998,385,386 ff.

205 Diese Argumentation dürfte sich indessen nach Inkrafttreten der DSGVO mit dem aus ihr folgenden Rollen- und Aufgabenverständnis nicht mehr vereinbaren lassen. Denn nach den Artt. 37 ff. DSGVO nimmt der Datenschutzbeauftragte, weisungsfrei und unabhängig von der Geschäftsleitung, weder unternehmerische noch behördliche Aufgaben wahr. Institutionell verfolgt nicht nur Arbeitgeber-, sondern gerade auch Arbeitnehmerinteressen. Seine gesetzlichen Geheimhaltungs- und Vertraulichkeitsverpflichtungen gelten sowohl im Verhältnis zum Verantwortlichen als auch gegenüber sämtlichen internen Bereichen und Personen. Sie sind Grundlage und Voraussetzung für eine ordnungsgemäße Aufgabenwahrnehmung. Wenn und soweit Zweifel daran bestehen, dass der Datenschutzbeauftragte die entsprechende Qualifikation bzw. Fähigkeit erfüllt, kann und darf er dieses Amt nicht ausüben. Umgekehrt kann es, wenn und soweit er es ausübt, keine „abgestufte" Verantwortung geben, von der einzelne Bereiche ganz oder teilweise ausgenommen und deshalb kontrollfrei sind. Und das BetrVG schließlich kann als nationales Gesetz die generellen und verbindlichen Vorgaben der DSGVO nicht modifizieren.

206 Daher ist der betriebliche Datenschutzbeauftragte nach Art. 39 Abs. 1 DSGVO auch berechtigt und verpflichtet, die Mitarbeitervertretung zu beraten und deren Datenverarbeitung zu überwachen. Davon unberührt bleiben selbstverständlich die eigenen Rechte und Pflichten der Mitarbeitervertretung, auch soweit sie sich auf datenschutzrechtlich relevante Vorgänge beziehen. Sie muss sich einer datenschutzrechtlichen Bewertung des Datenschutzbeauftragten nicht anschließen, und sie nimmt ihre Beteiligungsrechte unabhängig von diesem wahr. Zugleich ist die Mitarbeitervertretung weder berechtigt noch verpflichtet, den Datenschutzbeauftragten zu kontrollieren. Die Unternehmensleitung wiederum hat keinen Anspruch darauf zu erfahren, was der Datenschutzbeauftragte mit der Mitarbeitervertretung erörtert oder bei geprüft hat und zu welchem Befund er gelangt ist, wenn und soweit sich der Datenschutzbeauftragte nicht seinerseits im Rahmen seiner Unabhängigkeit zu einem entsprechenden Bericht entschließt.

207 Eine weitere Frage in diesem Zusammenhang bezog sich auf die **Weitergabe personenbezogener Daten Freier Mitarbeiter** an die Mitarbeitervertretungen. Hintergrund ist, dass in einigen Rundfunkanstalten die Interessen dieses Personenkreises – soweit es sich dabei um arbeitnehmerähnlich Beschäftigte im Sinne des § 12 TVG handelt – entweder vom jeweiligen Personalrat oder anstelle des Personalrats von einer institutionalisierten Freienvertretung wahrgenommen werden. Grundlage sind im ersten Fall entsprechende pauschale Zuständigkeitsverweise des jeweiligen Personalvertretungsgesetzes, im zweiten Fall ein auf gesetzlicher bzw. staatsvertraglicher Grundlage in Kraft gesetztes Freienstatut der jeweiligen Rundfunkanstalt.

208 In datenschutzrechtlicher Hinsicht entscheidend ist in beiden Fällen, welche personenbezogenen Daten die Interessenvertretung benötigt, um die ihr durch das je-

weilige Regelwerk übertragene Aufgabe wirksam wahrnehmen zu können. Dies hängt von einer Beurteilung der jeweiligen Aufgabe und der damit verbundenen Verarbeitungszwecke ab. Insbesondere ist also jeweils zu prüfen, ob die Mitarbeitervertretung die ihr übertragene Aufgabe jeweils nur auf der Grundlage personenbezogener Datenbestände sinnvoll ausüben kann, oder ob dafür beispielsweise auch pseudonymisierte bzw. anonymisierte bzw. statistische Daten genügen. Auch über den Umfang der jeweils zur Verfügung zu stellenden personenbezogenen Datenbestände ist abhängig von der jeweiligen konkreten Aufgabe und dem konkreten Anlass zu entscheiden.

209 Ob der jeweilige Beteiligungstatbestand in einem Personalvertretungsgesetz oder in einem auf gesetzlicher Grundlage verabschiedeten Freienstatut verankert ist, spielt dabei für diese Abwägung keine Rolle; insbesondere hat der Personalrat also insoweit aus datenschutzrechtlicher Sicht keine weitergehenden Ansprüche bzw. Befugnisse als eine Freienvertretung. Denn in beiden Fallkonstellationen ist zu berücksichtigen, dass sich die Beschäftigtengruppe der arbeitnehmerähnlichen Personen strukturell von der der Festangestellten dadurch unterscheidet, dass sie an den Auftraggeber weniger eng gebunden ist als ein Arbeitnehmer an den Arbeitgeber. Daher unterscheiden sich auch die wechselseitigen Loyalitäts-, Verhaltens- und Duldungspflichten der jeweiligen Beschäftigtengruppen voneinander. Dies gilt umso mehr, als sich der Status der „Arbeitnehmerähnlichkeit“ immer wieder ändern kann. Den damit verbundenen Besonderheiten muss der Arbeit- bzw. Auftraggeber bzw. müssen die Mitarbeitervertretungen zwingend Rechnung tragen, und zwar unabhängig davon, ob es sich um eine herkömmliche Belegschaftsvertretung wie den Personal- oder Betriebsrat oder eine neue, spezifische wie die Freienvertretung handelt. Dementsprechend muss selbst dort, wo ein Personalvertretungsgesetz ohne weitere Differenzierung für die Personengruppe der arbeitnehmerähnlich Beschäftigten für anwendbar erklärt wird, der Arbeitgeber in Bezug auf jeden Beteiligungstatbestand und in jedem Einzelfall prüfen, ob und inwieweit er dem Personalrat auf seiner Grundlage – und damit ohne deren jeweiliges Einverständnis - personenbezogene Daten dieser Beschäftigten(gruppe) überlassen darf. Die Möglichkeit einer Weitergabe dieser Daten mit dem Einverständnis der Betroffenen bleibt davon selbstverständlich stets unberührt.

210 Schließlich ging es noch um die Frage, wie der Arbeitgeber wirksam das Einverständnis für die **Nutzung von Mitarbeiterfotos für Zwecke der Öffentlichkeitsarbeit** einholen kann. Die Voraussetzungen dafür ergeben sich aus Art. 4 Nr. 11 und Art. 7 Abs. 2, 4 DSGVO. Danach ist eine der Aufnahme und seiner Veröffentlichung vorausgehende freiwillige, informierte, bestimmte und förmliche Einwilligung der betreffenden Person erforderlich. Die Hürden für eine im engeren Sinne freiwillige Einwilligung liegen dabei im Beschäftigungskontext wegen des typischerweise bestehenden Abhängigkeitsverhältnisses (§ 26 Abs. 2 BDSG) deutlich höher als in sonstigen Rechtsverhältnissen. Im konkreten Fall hatte der Verant-

wortliche allerdings ein Verfahren gewählt, das nach meiner Beurteilung die Gewähr für einen datenschutzrechtlich zulässigen Einsatz der Mitarbeiterfotos für die vorgesehenen Werbemaßnahmen bot.

k Status des internen DSB

211 Die aufsichtsrechtliche Beurteilung datenschutzrechtlicher Sachverhalte ist nach der Logik des Datenschutzzuständigkeits- und -verfahrensregimes die Ausnahme, die Regel hingegen der „operative" Datenschutz vor Ort. Zu den in der Praxis bedeutsamsten Themen gehört dabei die Aufgabenverteilung zwischen dem datenschutzrechtlich „Verantwortlichen" und dem internen Datenschutzbeauftragten.

212 Die dafür maßgeblichen Rahmenvorgaben ergeben sich unmittelbar aus der DSGVO. Deren Verhaltens- und Handlungsvorgaben zur Gewährleistung des Datenschutzes in der Praxis richten sich sämtlich an den „Verantwortlichen" (Art. 4 Nr. 7 DSGVO); das gilt auch für die Benennung des Datenschutzbeauftragten. Dessen Stellung legt Art. 38, seinen Aufgabenbereich Art. 39 DSGVO fest. Die entsprechenden Vorschriften gelten, gleich ob der Verantwortliche gemäß Art. 37 DSGVO verpflichtet ist, einen Datenschutzbeauftragten zu benennen, oder dies freiwillig tut (s. bereits oben Rn. 101), ob es sich um eine beauftragte externe Person oder einen intern Beschäftigten handelt, und ob diese Person ausschließlich diese Funktion oder auch noch eine andere wahrnimmt; im letztgenannten Fall dürfen die sich daraus ergebenden Rechte und Pflichten nicht zu einem Interessenkonflikt führen, Art. 38 Abs. 6 DSGVO. Zwingend muss der Verantwortliche gemäß Art. 38 Abs. 3 DSGVO dafür sorgen, dass der Datenschutzbeauftragte in dieser Rolle weisungsfrei bleibt und ihretwegen nicht benachteiligt wird, Art. 38 Abs. 3 DSGVO.

213 Zu den Aufgaben des DSB gehört es, den Verantwortlichen zu unterrichten und zu beraten, die Einhaltung der Datenschutzvorgaben und der Datenschutzstrategien des Verantwortlichen zu überwachen und mit der Aufsichtsbehörde zusammenzuarbeiten, Art. 39 Abs. 1 DSGVO. Der Verantwortliche wiederum muss ihn frühzeitig in alle insoweit relevanten Vorgänge einbinden und ihn organisatorisch unterstützen, Art. 38 Abs. 1 und 2 DSGVO.

214 Insgesamt ergibt sich daraus das Bild einer Beratungs-, Unterstützungs- und Überwachungsinstanz, über deren Einrichtung und Ausstattung zwar zunächst der Verantwortliche entscheidet, die in ihrer darauf basierenden Funktion aber von ihm unabhängig agiert. Diese Unabhängigkeit ist nur gewährleistet, wenn der Datenschutzbeauftragte nicht in die Situation kommt, unmittelbar oder mittelbar eigenes Handeln überwachen zu müssen. Dies würde zu einem unzulässigen Interessenkonflikt führen, den Art. 38 Abs. 6 S. 2 DSGVO ausdrücklich verbietet. Zwar benennt diese Regelung nur den Fall, dass der DSB auch noch weitere Aufgaben für den

Verantwortlichen wahrnimmt, wie dies in der Praxis häufig – im Rahmen von Teilzeitkonstruktionen – geschieht. Dies liegt aber nur daran, dass insoweit die Gefahr eines Interessenkonflikts besonders nahe liegt. Das Verbot selbst gilt generell.

215 Daher darf der Datenschutzbeauftragte weder freiwillig noch gar auf Anweisung des Verantwortlichen Aufgaben übernehmen, die der Umsetzung der diesem obliegenden Handlungs- und Gewährleistungspflichten dienen. So darf er beispielsweise weder selbst technisch-organisatorische Maßnahmen festlegen bzw. umsetzen (Art. 24 DSGVO), noch das Verzeichnis von Verarbeitungstätigkeiten führen (Art. 30 DSGVO) oder die Verantwortung für die Meldung nach Art. 33 DSGVO tragen. Dies kann im Einzelfall Abgrenzungsfragen aufwerfen. Da bei einem Dissens einseitige Anordnungen des Verantwortlichen stets die Gefahr einer Kollision mit dem Weisungsverbot nach Art. 38 Abs. 3 S.1 DSGVO begründen, ist es diesem grundsätzlich zu empfehlen, alle für die Funktion des internen DSB maßgeblichen Rahmenbedingungen schon vorab abstrakt-generell (z.B. in einer Datenschutzrichtlinie) und/oder im Zuge der Besetzung der Position vertraglich festzuhalten. Dies empfiehlt sich auch mit Blick auf das Verhältnis zwischen Aufgabenumfang und Ressourcen des Datenschutzbeauftragten, insbesondere soweit er die Aufgabe beispielsweise nur in Teilzeit wahrnimmt.

I Meldungen nach Art. 33

216 Nach Art. 33 DSGVO ist der Verantwortliche (oder Auftragsverarbeiter) verpflichtet, eine ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten der Aufsicht unverzüglich und möglichst binnen 72 Stunden zu melden, es sei denn, dass sie voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt[67]. Dabei ist es zunächst stets Sache des Verantwortlichen zu prüfen, ob die Voraussetzungen eines meldepflichtigen Vorgangs und der in den Fällen des Art. 34 DSGVO vorgeschriebene Benachrichtigung davon betroffener Personen vorliegen. Damit trägt er auch das Risiko eines etwaigen schuldhaften und gegebenenfalls aufsichtsrechtlich sanktionierten Unterlassens. In Zweifelsfällen sollte der Verantwortliche daher die Aufsicht benachrichtigen.

217 Im Jahr 2019 haben mich mehrere solcher Meldungen erreicht. In allen Fällen hat der jeweils Verantwortliche rasch und umsichtig reagiert und adäquate Maßnahmen ergriffen, um den Schaden zu begrenzen und die Wiederholung eines solchen Vorfalls zu vermeiden. Nur in einem Fall war die betroffene Person zu benachrichtigen. Einige Vorfälle gingen auf Attacken mit Schadsoftware (Emotet) zurück; zu weitergehenden Schäden kam es dabei nicht. In drei Fällen habe ich von einer der Abhilfebefugnisse gemäß Art. 58 Abs. 2 lit. b) bzw. d) Gebrauch gemacht.

[67] S. dazu Kurzpapier Nr. 18 der DSK, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf

218 Da die Frist zur Meldung mit 72 Stunden sehr knapp, der Umfang der mit der Meldung anzugebenden Informationen nach Art. 33 Abs. 2 DSGVO hingegen ziemlich groß bemessen ist, habe ich ein eigenes Meldeformular mit erläuternden Hinweisen entwickelt, um den Verantwortlichen in meinem Zuständigkeitsbereich diese Arbeit zu erleichtern. Es ist lediglich als Handreichung zu verstehen und auf meiner Homepage zugänglich[68].

5 Auftragsverarbeitung

219 Außer im Bereich der Datenverarbeitung für journalistische Zwecke, für die die entsprechenden Regelungen gemäß § 9c Abs. 1 S. 4 RStV nicht gelten (s. bereits oben Rn. 172), erstreckt sich meine Aufsichtszuständigkeit nicht nur auf die Verantwortlichen, sondern auch auf die von ihnen beauftragten Auftragsverarbeiter. Dies bedeutet, dass sich sowohl die Aufgaben nach Art. 57 als auch die Befugnisse nach Art. 58 DSGVO auf den von Seiten eines Verantwortlichen eingeschalteten Auftragsverarbeiter beziehen.

220 Die Abgrenzung zwischen gemeinsamer Verantwortung im Sinne von Art. 26 DSGVO und Auftragsverarbeitung gemäß Art. 28 DSGVO kann in der Praxis zu einigen Schwierigkeiten führen. Sie sind nicht nur relevant mit Blick auf die Rechtsprechung des EuGH zum Verständnis der gemeinsamen Verantwortlichkeit etwa im Zusammenhang mit der Einbindung von Drittplattformen auf eigenen Online-Angeboten sowie die damit verbundenen Informationspflichten (s. bereits oben Rn. 172 ff.), sondern auch für die Reichweite der Aufsichtszuständigkeit. Zumindest für eine allgemeine Orientierung können zwei Kriterien dienen[69]: Formal geht es um eine Auftragsverarbeitung, wenn nur einer der Beteiligten über die Verarbeitungszwecke entscheidet und dem oder den anderen insoweit Weisungen erteilen kann. Und inhaltlich steht im Auftragsverarbeitungsverhältnis die Verarbeitung des Bestands an personenbezogenen Daten des Verantwortlichen im Mittelpunkt, nicht eine sonstige Dienstleistungsfunktion, die lediglich eine solche Verarbeitung zur Folge hat.

221 Im Jahr 2019 war ich mit mehreren – in einem Fall auch: miteinander verbundenen - Auftragsverarbeitungsverhältnissen befasst. In einem von ihnen gab es deutliche Anzeichen für eine datenschutzwidrige Praxis des Auftragsverarbeiters, der ich allerdings nicht mehr nachgehen musste bzw. auf die ich nicht mehr reagieren konnte,

---

68 https://www.rundfunkdatenschutz.de/datenschutzerklaerung/datenschutzerklaerung.html

69 Siehe im übrigen das Kurzpapier Nr. 13 der DSK, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

weil das zugrunde liegende Vertragsverhältnis ohnehin zum Jahresende auslief. Außerdem war die für den Auftragsverarbeiter zuständige staatliche Aufsichtsbehörde über diese Praxis ebenfalls informiert.

6 Kontrollen und Prüfungen

222 In die Zuständigkeit des Rundfunkdatenschutzbeauftragten fällt es gemäß Art 51 Abs 1 und Art 58 Abs 1b DSGVO, die Umsetzung der DSGVO bei den Verantwortlichen zu prüfen. Dies muss nicht immer auf einen Anlass, bspw. eine Beschwerde zurückgehen, sondern soll ab 2020 auch in Form von geplanten Audits stattfinden. Im Jahr 2019 bestand für eine solche Prüfung mit Blick auf den vorrangigen Handlungsbedarf zum Aufbau der Aufsichtsstruktur und -organisation weder Zeit noch Anlass.

223 Für die Jahre 2020 bis 2022 jedoch habe ich ein Auditprogramm entworfen, in dem risikobasierte Schwerpunktthemen festgelegt sind. Die Verantwortlichen werde ich mit angemessener Frist vor der Prüfung über den jeweiligen Gegenstand, die Zielsetzung und den maßgeblichen Umfang der Prüfung informieren. Parallel ist für das Jahr 2020 eine allgemeine Abfrage zur Umsetzung der DSGVO im Beteiligungsbereich der Rundfunkanstalten in meinem Zuständigkeitsbereich vorgesehen, ähnlich wie dies in der Vergangenheit bereits staatliche Aufsichtsbehörden hinsichtlich der ihrer Aufsicht unterliegenden kleineren und mittleren Unternehmen unternommen haben.

7 Zahlen und Fakten 2019

224 Nach Art. 59 DSGVO kann der Jahresbericht über die Tätigkeit der Aufsichtsbehörde eine Liste der Arten der gemeldeten Verstöße und der getroffenen Maßnahmen nach Art. 58 Abs. 2 DSGVO enthalten. Da ich mich zu den entsprechenden Anlässen und Reaktionen bereits im unmittelbaren Zusammenhang mit dem jeweiligen Thema geäußert habe, und angesichts ihrer vergleichsweise geringen Aussagekraft verzichte ich auf eine derartige Liste. Stattdessen sind im folgenden einige statistische Kenndaten meiner Tätigkeit im Jahr 2019 dargestellt.

Im ersten Amtsjahr war ich mit insgesamt 212 Vorgängen befasst, in denen sich außenstehende Dritte an mich gewandt haben. Berücksichtigt sind hierbei also die Aufgaben der Aufsicht im Außenverhältnis und nicht die Beratungs- und Konsultationsanfragen im Verhältnis zu den Verantwortlichen bzw. ihren Datenschutzbeauftragten in meinem Zuständigkeitsbereich. Ebenfalls nicht statistisch erfasst sind die

teilweise sehr umfangreichen Prüfvorgänge, mit denen ich in anderen Zusammenhängen befasst war.

225 Vor allem in der zweiten Jahreshälfte haben mich vermehrt Anfragen von außen erreicht, zum Jahresende nahm die Zahl der Eingaben wieder ab.

226 Erreichbar bin ich auf unterschiedlichen Wegen. Der überwiegende Anteil der Kontakte kommt per Mail zustande. Eine Umstellung der Kontakt-Seite auf meiner Homepage im letzten Quartal 2019 führte dazu, dass das Webformular stärker genutzt wurde. Die Zuschriften per Post oder Fax gingen hauptsächlich auf Beschwerden zurück. Auskunftsersuchen und Datenschutzvorfälle haben mich ausschließlich per Mail erreicht.

227 Vorbehaltlich abweichender Wünsche beantworte ich Anschreiben stets über das vom Petenten selbst gewählte Medium (Post, Fax, Mail). Dessen Kontaktaufnahme kann unterschiedlichste Gründe haben, die wir intern einer der folgenden Kategorien subsumieren.

228 **a) Beschwerde**
Hier reklamiert die betroffene Person, selbst von einer Datenschutzverletzung betroffen zu sein. Im Jahr 2019 hat knapp die Hälfte der Beschwerden den Rundfunkdatenschutzbeauftragten per Mail und knapp 40% per Fax erreicht. Hierauf erfolgten acht Bescheide und 21 Stellungnahmen. Zehn Beschwerden fielen nicht in mein Aufgabengebiet und acht Fälle waren zum Jahresende noch nicht final abgeschlossen.

229 **b) Anzeige**
Mit einer Anzeige reklamiert eine Person eine Datenschutzverletzung, die (im Gegensatz zur Beschwerde) nicht unmittelbar sie selbst betrifft. 2019 hat mich eine Anzeige erreicht, die ich mit einer Stellungnahme beantwortet habe.

230 **c) Beratungsanfrage**
In einer Beratungsanfrage werden allgemeine Fragen zum Datenschutz und der Handhabung von Daten bei den Rundfunkanstalten verstanden. 75% solcher Beratungsanfragen habe ich inhaltlich beantwortet, eine mit einem Bescheid. Die restlichen Beratungsanfragen wurden mit einem Verweis wegen Nichtzuständigkeit geschlossen.

231 **d) Datenschutz im Programm**
Die besondere Stellung des Datenschutzes im Programm (siehe Rn 8 ff.) ist vielen Petenten nicht hinreichend bekannt. 2019 erreichten mich dazu acht Anschreiben, von denen ich zwei an den Verantwortlichen verwiesen habe. Zum Jahreswechsel waren noch zwei Anfragen in Bearbeitung.

232 **e) Auskunftsersuchen**
Ebenso wie alle anderen Stellen, in denen Datenverarbeitung stattfindet, ist die Frage zu den erhobenen personenbezogenen Daten an den Rundfunkdatenschutzbeauftragten legitim. Ich bin hier ebenso auskunftspflichtig wie alle anderen verantwortlichen Stellen. Allerdings habe ich keinen Zugriff auf die Daten der Rundfunkbeitragsschuldner beim zentralen Beitragsservice, sondern verarbeite lediglich Daten im Zusammenhang mit der Bearbeitung von Einlassungen. Die Auskunft auf vier Ersuchen, die mich 2019 erreicht haben, habe ich fristgerecht übermittelt.

233 **f) Sonstiges**
Als eine der Aufsichtsbehörden für den zentralen Beitragsservice wird der Rundfunkdatenschutzbeauftragte oft in Bezug auf Kontenklärungen und Beschwerden bezüglich des Rundfunkbeitrags angeschrieben. Hierfür bin ich allerdings nicht zuständig und verweise die Petenten folglich an die Kontaktstellen der Rundfunkanstalten und des Beitragsservice. Nur in weniger als zwei Prozent habe ich mit einer Stellungnahme reagiert.

234 Im übrigen gebe ich jeden Vorgang mit Bezug zum Beitragsservice, in dem erkennbar erstmals ein allgemeines oder spezifisches datenschutzrechtliches Anliegen formuliert wird, an die dortige Datenschutzbeauftragte ab. Die Datenschutzaufsicht sehe ich nur in zweiter Linie gefragt, wenn es um allgemeine datenschutzrechtliche Erläuterungen geht. Entsprechendes gilt für Anfragen, die eine Rundfunkanstalt betreffen.

235 **g) Datenschutzvorfall**
Eine Verletzung der Datenschutzvorgaben ist hier als Datenschutzvorfall bezeichnet. Dieser kann durch die Verantwortliche Stelle selbst gemeldet werden oder aus einer durch eine Anzeige oder Beschwerde ausgelöste Untersuchung des Rundfunkdatenschutzbeauftragten hervor gehen.

236 2019 wurden mir acht Datenschutzvorfälle gemeldet, von denen ich für fünf unmittelbar zuständig war. Auf sie habe ich mit je zwei Bescheiden und zwei Stellungnahmen reagiert. Der verbliebene Fall befand sich am Jahresende noch in der Untersuchung.

237 **h) Vorabkonsultation und Beratung**

Die Verantwortlichen bzw. ihre Datenschutzbeauftragten haben sich 2019 mehrfach in unterschiedlicher Weise mit der Bitte um Beratung bzw. aufsichtsrechtliche Bewertung von Sachverhalten an mich gewandt. Eine verbindliche Stellungnahme habe ich nur im Rahmen der Vorab-Konsultation abgegeben.