Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten für das Jahr 2021

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

Der dritte Bericht über die Tätigkeit des gemeinsamen Rundfunkdatenschutzbeauftragten der drei ARD-Landesrundfunkanstalten Bayerischer Rundfunk, Saarländischer Rundfunk und Westdeutscher Rundfunk sowie des Deutschlandradio und des ZDF bietet wie gewohnt einen Überblick über die medienrelevanten Entwicklungen in Datenschutzrecht und Datenschutzpraxis sowie meine Tätigkeitsschwerpunkte im Jahr 2021. In erster Linie dient er dazu, Transparenz über die Erkenntnisse, Rechtsauffassungen und Aktivitäten der Datenschutzaufsichtsbehörde gegenüber der Öffentlichkeit herzustellen. Er ist damit eine kompakte Informationsquelle für alle Angelegenheiten mit Bezug zum Zuständigkeitsbereich des gemeinsamen Rundfunkdatenschutzbeauftragten.

Zugleich bietet mein Tätigkeitsbericht Orientierung in doppelter Hinsicht: Zum einen allen, die als von einer Datenverarbeitung (potentiell) Betroffene vorab prüfen wollen, ob sich ein Verantwortlicher in meinem Zuständigkeitsbereich datenschutzkonform verhält und sie sich beispielsweise mit Aussicht auf Erfolg mit einer Beschwerde an mich wenden können – sei es als Beitragszahlerin oder Beitragszahler, als Vertragspartnerin oder Vertragspartner einer Rundfunkanstalt oder eines ihrer Beteiligungsunternehmen oder als Hörerin, Zuschauer oder Onlinenutzerin. Zum anderen können sich die Verantwortlichen in meinem Zuständigkeitsbereich sowie alle sonstigen Verantwortlichen insbesondere im (öffentlich-rechtlichen) Rundfunk mithilfe meines Tätigkeitsberichts über etwaigen Beratungs-, Veränderungs- oder Handlungsbedarf vergewissern. Bewusst ist mein Tätigkeitsbericht deshalb auch im Sinne eines jahresübergreifenden Kompendiums aller relevanten Themen angelegt: Vielfach verweise ich auf ausführlichere Erläuterungen zu einzelnen Themen in einem meiner vorangegangenen Berichte, die ich im aktuellen Bericht nicht noch einmal aufgreife.

Schließlich soll der Tätigkeitsbericht aber nach Sinn und Zweck des Art. 59 DSGVO auch zur Meinungsbildung beitragen, Diskussionen anstoßen und Empfehlungen geben. Er ist damit eines der wenigen Mittel der Öffentlichkeitsarbeit, die dem Rundfunkdatenschutzbeauftragten (angesichts sehr begrenzter Kapazitäten) zur Verfügung stehen. Neben den zuvor bereits angesprochenen Adressaten richtet er sich insoweit primär an Akteure wie die für Datenschutz- und Rundfunkregulierung zuständigen Parlamente und Regierungen der Bundesländer sowie die Kollegialorgane der Rundfunkanstalten, denen der Tätigkeitsbericht jeweils zu erstatten ist.

Drei Jahre Praxiserfahrung belegen, dass die Mandatierung eines gemeinsamen Rundfunkdatenschutzbeauftragten ein Musterbeispiel einer in jeder Hinsicht sinnvollen Kooperation im öffentlich-rechtlichen Rundfunk ist, die zugleich die rundfunkspezifische Datenschutzaufsicht deutlich gestärkt hat. Gleichwohl kann die bisherige Konstruktion das Effizienz- und Durchsetzungspotential einer echten Strukturreform (in Gestalt einer Aufsichtsbehörde für mehrere oder – besser noch – alle Rundfunkanstalten) nicht vollständig ausschöpfen. Die Voraussetzungen dafür zu schaffen, wäre freilich Sache der Bundesländer.

Sophia Schulze Schleithoff danke ich herzlich für ihre große Unterstützung insbesondere beim letztjährigen Prüfvorhaben sowie bei der Schlussredaktion dieses Tätigkeitsberichts.

Potsdam, Februar 2022
Dr. Reinhart Binder

Inhaltsverzeichnis

Hinweise:

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 Der Rundfunkdatenschutzbeauftragte (im folgenden: RDSB) legt als Aufsichtsbehörde gemäß Art. 59 DSGVO einen Jahresbericht über seine Tätigkeit vor. Diesen hat er dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden zu übermitteln. Er ist der Öffentlichkeit, der Kommission und dem Europäischen Datenschutzausschuss (Art. 68 DSGVO) zugänglich zu machen.

2 Die für mich maßgeblichen Landesrundfunkgesetze bzw. Staatsverträge verweisen auf Art. 59 DSGVO und sehen im wesentlichen gleichlautend vor, dass der RDSB den Bericht jährlich „auch den Organen" der Rundfunkanstalt bzw. Körperschaft erstattet[1]. Ebenfalls gleichlautend fordern alle Vorschriften, wie von Art. 59 DSGVO vorgegeben, eine Veröffentlichung des Berichts, wobei sie eine solche im Onlineangebot der jeweiligen Rundfunkanstalt für ausreichend erklären. Eine Vorgabe 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. Letztlich handelt es sich dabei um eine eher deklaratorische und zudem – da die Belange der Beteiligungsunternehmen hier nicht angesprochen sind – unvollständige Vorgabe.

3 Mit Blick auf das auch für die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk maßgebliche Gebot der Staatsferne sind nach meinem Verständnis Adressaten meines Tätigkeitsberichts in erster Linie die (jeweils drei) Organe der fünf Rundfunkanstalten in meinem Zuständigkeitsbereich: Rundfunk-/Hörfunk-/Fernsehrat, Verwaltungsrat sowie Intendantin bzw. Intendant. Sie informiere ich förmlich ebenso über die Veröffentlichung des Berichts wie die jeweiligen Landesregierungen und -parlamente, darunter die der beiden für das ZDF und das Deutschlandradio jeweils aktuell rechtsaufsichtsführenden Länder. Abrufbar ist er in der Infothek meiner Homepage. Die Rundfunkanstalten können anstelle oder zusätzlich zu einer Veröffentlichung auf ihrer eigenen Website auch auf diese Fundstelle verweisen bzw. sie verlinken, um ihre gesetzlichen Informationsverpflichtungen zu erfüllen.

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

1 Datenschutz und Datenschutzaufsicht: Grundlagen

a Gesetzgebung

aa) Europa

4 Seit Jahren bemüht sich die EU-Kommission darum, die mittlerweile fast 20 Jahre alte Datenschutzrichtlinie für elektronische Kommunikation[2] durch eine EU-Verordnung abzulösen, die – im Gegensatz zu einer Richtlinie – in den Mitgliedstaaten unmittelbar gilt (s. dazu bereits TB 2020 Rn. 9). Diese sogenannte **ePrivacy-Verordnung** soll ergänzend zur DSGVO bzw. in Teilen über sie hinaus oder an ihrer Stelle Privatautonomie und Datenschutz bei der Nutzung elektronischer Kommunikation gewährleisten. Ein zustimmungsfähiger Entwurf ist allerdings auch in diesem Berichtsjahr nicht zustande gekommen.

5 Weiterhin gelten deshalb die Vorschriften der ePrivacy-Richtlinie. Sie verdrängen die Regelungen der DSGVO, soweit sie a) vergleichbare Regelungsziele wie sie verfolgen und b) in nationales Recht transformiert worden sind. In Deutschland war besonders umstritten, ob § 15 Abs. 3 Telemediengesetz (TMG) die Vorschriften der ePrivacy-Richtlinie vollständig in nationales Recht umsetzte. Davon hing ab, ob und unter welchen Voraussetzungen es zulässig war, mithilfe von Cookies Daten zur Nutzung von Onlineangeboten auch ohne Einwilligung der Betroffenen zu verarbeiten (s. dazu unten Rn. 117 ff.). Mit dem Inkrafttreten des § 25 TTDSG am 1. Dezember 2021 (unten Rn. 18 ff.) hat sich dieser Streit erledigt.

6 Zwei weitere große Gesetzgebungsvorhaben mit zumindest mittelbarem datenschutzrechtlichem Bezug hat die EU-Kommission indes mit Nachdruck vorangetrieben. Die Kommissionspräsidentin hat das Gesetzespaket zur Digitalstrategie „Ein Europa für das digitale Zeitalter" zu einem der Leuchtturmprojekte ihrer Amtsperiode erklärt. Bislang liegen die Vorbereitungen im selbstgesetzten Zeitplan:

7 Zum einen soll ein Digitale-Dienste-Gesetz (**Digital Services Act**[3]) Regeln „für ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld" schaffen, „in dem die in der Charta verankerten Grundrechte wirksam geschützt sind". Es zielt auf neue Rahmenbedingungen vor allem für die großen supranationalen Online-Plattformanbieter wie Facebook, Google oder Telegram, die mehr als 10 % der Bevölkerung in der EU erreichen. Es soll die Anbieter insbesondere verpflichten, kriminellen Aktivitäten bzw. illegalen Inhalten auf ihren Plattformen entgegenzuwirken.

8 Dies hat nicht zuletzt Konsequenzen für den Umgang mit den personenbezogenen Daten der Nutzer der von diesen Unternehmen angebotenen Dienste. Unter anderem sollen die Konzerne verpflichtet sein, den nationalen Behörden die von ihnen zusammengetragenen

---

2 Richtlinie (EU) 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), AmtsBl (EU) L 201 vom 31.07.2002.

3 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2003/31/EG vom 15.12.2020, COM (2020) 825 final, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0825.

Daten in bestimmten Fällen zur Verfügung zu stellen. Auch müssen sie Maßnahmen gegen missbräuchliche Inhalte ergreifen, Straftaten melden, Gegendarstellungen ermöglichen, und den Nutzern das Recht einräumen, auf Profiling beruhende Empfehlungen unterbinden zu können. Behörden und Wissenschaft sollen einen Zugang zu den Datenbeständen der Plattformbetreiber erhalten, um die Mechanismen viraler Phänomene und die Risiken für die Gesellschaft und die Grundrechte besser beurteilen zu können. Hingegen übernimmt der bis Ende 2021 entwickelte Vorschlag nicht die von vielen erhobene Forderung nach einem Anspruch darauf, die von den Plattformbetreibern angebotene Dienste auch anonym nutzen zu können. Auch die von Presseverbänden geforderten Ausnahme von der Pflicht zur Löschung problematischer Inhalte, wenn es sich dabei um „journalistische Inhalte" bzw. Pressepublikationen handelt, zeichnet sich nicht ab.

9 Im Verbund mit dem Digital Services Act soll es zudem ein Digitale-Märkte-Gesetz (**Digital Market Act**)[4] künftig unter anderem ermöglichen, die „Datenmacht" der Internetkonzerne als Marktvorteil zu qualifizieren und diese insoweit der Aufsicht einer neuen europäischen Behörde zu unterstellen. Bislang fehlen effektive Mittel, die supranationalen Konzerne dazu zu veranlassen, ihrem Geschäftsverhalten die Datenschutzstandards der EU zugrunde zu legen. Das liegt nicht zuletzt daran, dass viele Datenschutzbehörden der EU-Mitgliedstaaten faktisch nur bedingt willens oder in der Lage sind, die Vorgaben der DSGVO im Verhältnis zu diesen Konzernen durchzusetzen. Die EU sieht daher auch unter dem spezifischen Gesichtspunkt des Verbraucherschutzes noch Ergänzungs- und Handlungsbedarf.

10 Der zum 1. Januar 2021 vollzogene **Brexit** hingegen hat zumindest in datenschutzrechtlicher Hinsicht keine Defizite hinterlassen. Kurz vor Ablauf der sechsmonatigen Übergangsfrist stellte die EU-Kommission am 28. Juni 2021 in einem sogenannten Angemessenheitsbeschluss fest, dass das Datenschutzniveau im Vereinigten Königreich dem der DSGVO entspreche[5]. Damit dürfen die Verantwortlichen in Deutschland personenbezogene Daten weiterhin ohne zusätzliche vertragliche Absprachen bzw. Garantien nach Art. 46 DSGVO in das Vereinigte Königreich übermitteln. Wie jeder Angemessenheitsbeschluss gilt auch dieser für zunächst vier Jahre, also bis Mitte 2025.

bb) Deutschland

11 In Deutschland traten im Laufe des Jahres 2021 mehrere datenschutzrechtlich relevante Gesetze in Kraft. Besonders umstritten war die geplante Novellierung des Rechts zur **Bestandsdatenauskunft**, nachdem das BVerfG die zugrunde liegende Vorschrift des § 113 Telekommunikationsgesetz (TKG) im Mai 2020 für verfassungswidrig erklärt (TB 2020 Rn. 30) und damit zugleich mittelbar das geplante Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität aufgehalten hatte (TB 2020 Rn. 12), das auf den Regeln zur Bestandsdatenauskunft basiert. Die entsprechenden Vorschriften ermöglichen es Si-

---

4 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) vom 15.12.2020, COM (2020) 842 final, https://eur-lex.europa.eu/legal-content/de/TXT/?uri=COM:2020:842:FIN.

5 Durchführungsverordnung (EU) 2021/1772 der Kommission vom 28. Juni 2021, AmtsBl (EU) L 360/1 vom 11.10.2021; siehe auch unten 32

cherheitsbehörden, von Telekommunikationsunternehmen Informationen etwa über den Inhaber eines Telefonanschlusses oder eine zu einem bestimmten Zeitpunkt zugewiesene IP-Adresse zu erhalten. Mitzuteilen sind ihnen dann personenbezogene Daten des Kunden, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen („Bestandsdaten"), nicht hingegen jene, die sich auf die Nutzung des betreffenden Dienstes oder den Kommunikationsinhalt beziehen („Verkehrsdaten"). Sowohl die Übermittlung der Daten durch den Telekommunikationsanbieter als auch deren Abruf durch die Behörden muss auf einer hinreichend konkreten und den Verhältnismäßigkeitsgrundsatz wahrenden Rechtsgrundlage beruhen.

12 Mit mehreren vom Vermittlungsausschuss durchgesetzten Modifikationen trat das Änderungsgesetz mit der Neufassung von § 113 TKG (inzwischen: § 174 TKG) sowie der einschlägigen Sicherheitsgesetze am 2. April 2021 in Kraft. Insbesondere kommt nun eine Passwortherausgabe gegenüber Ermittlungsbehörden nur im Falle des Verdachts besonders schwerer Straftaten in Betracht, und Telemediendienstanbieter sind zur Auskunft zu den ihnen vorliegenden Bestandsdaten nur verpflichtet, wenn es um die Verfolgung besonders gewichtiger Ordnungswidrigkeiten geht.

13 Ferner ist am 11. Juni 2021 das **Gesetz zur Harmonisierung des Verfassungsschutzrechts** in Kraft getreten (dazu bereits TB 2019 Rn. 38 sowie TB 2020 Rn. 15). 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. Es erlaubt den Verfassungsschutzbehörden im Rahmen der sogenannten „Quellen-Telekommunikationsüberwachung" neben dem Abhören von Telefonaten und dem Zugriff auf SMS auch das Mitlesen von Chats auf Smartphones, bevor sie verschlüsselt werden.

14 Ermöglicht wird dies durch den Einsatz sogenannter „**Staatstrojaner**". Allerdings sehen die gesetzlichen Grundlagen keine spezifischen Vorkehrungen für Kommunikationsvorgänge im Zusammenhang mit journalistischer Tätigkeit – also journalistische Datenverarbeitung – vor. Sie überlassen es im Ergebnis den Sicherheitsbehörden zu bewerten, ob es um einen solchen geht. Daher ist fraglich, ob die weit gefassten Vorschriften mit dem vom „Medienprivileg" geschützten Redaktionsgeheimnis bzw. der durch Art. 5 Abs. 1 S. 2 GG garantierten Presse- und Rundfunkfreiheit vereinbar sind. Denn es ist zu befürchten, dass entsprechende Aktionen auch investigative Recherchen oder den Informantenschutz gefährden. Die Organisation „Reporter ohne Grenzen" hat dazu gemeinsam mit anderen Beteiligten – darunter auch einem für den WDR tätigen Investigativjournalisten - verwaltungsgerichtliche Verfahren eingeleitet. Ziel ist es, ein Verbot des Einsatzes von „Staatstrojanern" durch die Sicherheitsbehörden gegen Personen zu erwirken, wenn diese (im Rahmen ihrer journalistischen Tätigkeit) lediglich unverdächtige Nebenbetroffene eines solchen Kommunikationsvorgangs sind.

15 Im engen Zusammenhang damit steht die Novellierung des Gesetzes über den Bundesnachrichtendienst (**BND-Gesetz**). Dieses hatte das BVerfG im Mai 2020 ebenfalls in Teilen für verfassungswidrig erklärt und eine Überarbeitung bis Ende 2021 vorgegeben (TB 2020 Rn. 32). Das BVerfG erkannte zwar mit Blick auf die Gefahren international operierender krimineller Organisationen die große Bedeutung eines effektiven Datenzugriffs im Rahmen

einer strategischen Telekommunikationsüberwachung an. Zugleich hob es aber hervor, dass entsprechende Eingriffe in den Schutzbereich von Art. 10 Abs. 1 GG nur nach Maßgabe spezifischer Verfahrensregelungen und Kontrollmechanismen zulässig seien. Es betonte die besonderen Anforderungen, die dabei an den Schutz von Vertraulichkeitsbeziehungen zu stellen sind - insbesondere jene zwischen Journalisten und ihren Informanten. Unter anderem gegenüber dieser Berufs- und Personengruppe müsse deshalb eine gezielte Überwachung von vornherein begrenzt sein. Eine Überwachung ist danach nur zur Aufklärung schwerwiegender Gefahren und besonders schwerer Straftaten bzw. zur Ergreifung bestimmter gefährlicher Straftäter zulässig. Außerdem muss das öffentliche Interesse an der Information das Interesse der Betroffenen an dem Schutz der Vertraulichkeit im Einzelfall überwiegen. Und schließlich muss der Gesetzgeber diesen Schutz jedenfalls grundsätzlich durch eine „gerichtsähnliche ex ante-Kontrolle" absichern[6] .

16 Zentraler Bestandteil des novellierten BND-Gesetzes ist daher die Einrichtung eines Unabhängigen Kontrollrats, der die gesamte technische Aufklärung durch den BND kontrolliert. Die Neufassung ist in Teilen am 22. April 2021 und im übrigen am 1. Januar 2022 in Kraft getreten.

17 Am 28. Mai 2021 ist das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz 2.0**)[7] in Kraft getreten. Es erweitert die Prüf- und Kontrollbefugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowohl gegenüber der Bundesverwaltung als auch gegenüber Telekommunikations- und Telemedienunternehmen, IT-Produktherstellern sowie Betreibern „**kritischer Infrastrukturen**" (KRITIS). Zu diesen hatte der im Jahr 2019 bekannt gewordene Referentenentwurf noch pauschal Anlagen oder Teile davon zählen wollen, „die dem Bereich Kultur und Medien angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind". Dies hätte unmittelbar den öffentlich-rechtlichen Rundfunk in Deutschland betroffen (dazu ausführlich TB 2019, Rn. 36 f.). Eine dahingehende Vorschrift enthält die Neufassung zurecht nicht mehr. Ebenfalls ist entgegen der ursprünglichen Fassung keine Speicherpflicht für Systeme zur Angriffserkennung (dazu TB 2019, Rn. 160 ff.) mehr vorgesehen. Jedoch darf das BSI nunmehr Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes – also beispielsweise bei telefonischen oder Online-Kontakten mit Bundesbehörden - anfallen, bis zu 18 Monaten speichern. Im Fall einer Störung kann es außerdem von den Betreibern „kritischer Infrastrukturen" die Herausgabe bestimmter Informationen und personenbezogener Daten verlangen, § 8b Abs. 4a BSI-Gesetz.

18 Seit 1. Dezember 2021 schließlich gilt das Telekommunikations-Telemedien-Datenschutzgesetz (**TTDSG**). Es soll die Rechtsunsicherheit beseitigen, die durch das ungeklärte Verhältnis zwischen den Vorschriften der DSGVO und ePrivacy-Richtlinie einerseits sowie des Telemediengesetzes (TMG) und TKG andererseits in Bezug auf den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien entstanden ist, nicht zuletzt auch mit Blick auf die Rechtsprechung des Bundesgerichtshofs zur Auslegung von § 15 Abs. 3 TMG (TB 2020 Rn. 32 f.). Es fasst nun alle einschlägigen Datenschutzbe-

6 BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 -, Rn. 194, 257.
7 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18.05.2021, BGBl I Nr. 25 vom 27.5.2021.

stimmungen in einem Regelwerk zusammen und erleichtert damit den Verantwortlichen wie auch Nutzern den Überblick. Es wird allerdings nur so lange gelten, bis die EU die ePrivacy-Verordnung verabschiedet hat (oben Rn. 4), die dann (wie die DSGVO) unmittelbar in allen Mitgliedstaaten verbindlich wäre.

19 Die größte praktische Bedeutung hat wohl die Vorschrift des **§ 25 TTDSG**.[8] Sie setzt nun, anders als die Vorgängerregelung in § 15 TMG, nahezu wortidentisch die Vorgabe von Art. 5 Abs. 3 ePrivacy-Richtlinie um. Auf ihrer Grundlage ist der Einsatz von Cookies und vergleichbarer technischer Instrumente (wie etwa Pixel oder das sog. Fingerprinting) grundsätzlich nur noch zulässig, wenn sich der Nutzer vorher ausdrücklich damit einverstanden erklärt hat. Die bisherigen Ausnahmeregelungen des § 15 TMG sind entfallen. Stattdessen nennt § 25 Abs. 2 TTDSG nur noch zwei Fälle, in denen eine Einwilligung entbehrlich ist (dazu ausführlich unten Rn. 120 ff.). Die Einwilligung selbst muss in Art. 7 DSGVO definierten und vom EuGH entwickelten Anforderungen erfüllen. Bei alledem kommt es nicht darauf an, ob es um personenbezogene Daten geht: die ePrivacy-Richtlinie und damit auch § 25 TTDSG schützt die Privatsphäre und geht deshalb über den Anwendungsbereich der DSGVO hinaus, die das Grundrecht auf Datenschutz sichert.

20 Daraus ergeben sich auch Fragen zur **Aufsichtszuständigkeit**. Denn die Datenschutzaufsichtsbehörden sind grundsätzlich nur zur Überwachung datenschutzrechtlicher Vorgaben berechtigt. Zu diesen gehören aber keine Vorschriften, die unabhängig von der Verarbeitung personenbezogener Daten die Privatautonomie wahren sollen. Deshalb erweitert § 29 Abs. 2 TTDSG ausdrücklich die Zuständigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auf alle Fälle, in denen es um die Einhaltung von § 25[9] TTDSG „durch Anbieter von Telekommunikationsdiensten oder durch öffentliche Stellen des Bundes“ geht. Allerdings definiert das TTDSG den Begriff des „Anbieters von Telekommunikationsdiensten“ nicht, sodass die Frage entstehen könnte, ob darunter auch Einrichtungen wie die Rundfunkanstalten oder ihre Beteiligungsunternehmen zu subsumieren sind, soweit sie beispielsweise ein Corporate Network zur Verfügung stellen. Jedoch wäre

---

[8] § 25 Schutz der Privatsphäre bei Endeinrichtungen
(1) Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 2016/679 zu erfolgen.
(2) Die Einwilligung nach Absatz 1 ist nicht erforderlich,
1. wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder
2. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

[9] Die Vorschrift verweist auf § 24 anstatt auf § 25. Dabei kann es sich jedoch, wie aus der Entwurfsfassung hervorgeht, nur um ein Redaktionsversehen handeln. Dieses dürfte darauf zurückzuführen sein, dass der Bundestag das Gesetz unter größtem Zeitdruck in der letzten Lesung noch modifiziert und ergänzt hat.

der Bund schon kompetenzrechtlich nicht befugt, die landesrechtlichen Vorschriften über die Zuständigkeit für die Datenschutzaufsicht im Rundfunk- bzw. im Telemedienbereich auf diese Weise zu unterlaufen bzw. zu ändern. Gleichwohl habe ich für die Rundfunkdatenschutzkonferenz (RDSK) im Rahmen der Anhörung zum Gesetzesentwurf eine entsprechende Klarstellung angeregt. Dazu ist es indessen nicht gekommen. § 1 Abs. 1 Nr. 8 TTDSG stellt lediglich fest, dass „bei Telemedien" die Aufsicht durch die nach Landesrecht zuständigen Behörden unberührt bleibt; zu ihnen gehören auch die Rundfunkdatenschutzbeauftragten. Darüber hinausgehenden Klarstellungsbedarf hat der Bundesgesetzgeber offenbar nicht gesehen.

21 Nicht beantwortet ist damit allerdings die weitere Frage, wer – anstelle des Bundesdatenschutzbeauftragten – auf der Landesebene für die Aufsicht über die auch datenschutzrechtlich relevanten Vorgaben der §§ 19 ff. TTDSG zuständig ist. Denn Aktivitäten öffentlicher Stellen der Länder kann der Bundesdatenschutzbeauftragte zwar ebenso wenig beaufsichtigen wie solche der Rundfunkanstalten (ausgenommen die der Deutschen Welle) und ihrer Beteiligungsunternehmen. Aber die Landesdatenschutzbehörden – einschließlich der Rundfunkdatenschutzbeauftragten – dürften ihrerseits ohne entsprechende Gesetzesgrundlage nicht ohne weiteres befugt sein, Vorschriften zum Schutz der Privatsphäre zu überwachen und Verstöße dagegen zu sanktionieren. Um zu vermeiden, dass Zuständigkeiten unklar oder Bescheide zur Sanktionierung von Verstößen gegen die §§ 19 ff. TTDSG formell angreifbar sind, sollten die Bundesländer daher vorsorglich die Zuständigkeitsregelungen auch für den Rundfunkdatenschutzbeauftragten (ebenso wie die der anderen Aufsichtsbehörden auf Landesebene) um den Hinweis auf die §§ 19 bis 25 TTDSG ergänzen. Dies ist, soweit ersichtlich, bislang noch in keinem Bundesland geschehen.

22 Seit dem 22. September 2021 stellt **§ 126a StGB** das „Gefährdende Verbreiten personenbezogener Daten" unter Strafe[10] und ist damit ein Anwendungsfall des ansonsten weitgehend im BDSG (§§ 41 f. BDSG) verankerten Datenschutzstrafrechts. Im Mittelpunkt stehen dabei sogenannte „**Feindeslisten**", die in zunehmendem Maße in einschlägigen – vorwiegend rechtsextremen - Onlineforen bzw. Chatgruppen kursieren. Wenn dabei nicht allgemein zugängliche Daten in einer Art und Weise verbreitet werden, die die betroffene Person strafrechtlich relevanten Gefahren aussetzt, kann dies mit Freiheitsstrafe bis zu drei, im Falle allgemein zugänglicher Daten mit bis zu zwei Jahren bestraft werden. Allerdings gilt dies nur für jene, die die Daten „öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts" gem. § 11 Abs. 3 StGB – also in Schriften, auf Ton- oder Bildträgern, in Datenspeichern, Abbildungen etc. oder unabhängig von einer Speicherung mittels Informations- oder Kommunikationstechnik - verbreiten. Dies wirft die Frage auf, ob sich das Verbot auch auf die Verbreitung in geschlossenen, aber mitgliederstarken Messengergruppen wie vor allem bei Telegram erstreckt. Problematisch ist in jedem Fall, dass sich der Straftatbestand damit auch auf journalistisch veranlasste Beiträge beziehen kann. Eine dahingehende Anwendung der Vorschrift wäre allerdings mit der durch Art. 5 Abs. 1 S. 2 GG garantierten Rundfunk- bzw. Pressefreiheit nicht vereinbar.

23 Zunehmend setzt sich die Erkenntnis durch, dass **personenbezogene Daten ein Wirtschaftsgut** und der wertvollste Rohstoff unzähliger neuer Geschäftsmodelle sind. Dies

[10] ÄndG zum StGB vom 14.9.2021, BGBl I S. 4250 vom 21.9.2021.

schlägt sich nun auch in unterschiedlichen Gesetzgebungsvorhaben auf europäischer (oben Rn. 9) und nationaler Ebene nieder.

24 Schon im Januar 2021 trat die sogenannte kartellrechtliche Digitalisierungsnovelle in Kraft. So sanktioniert nunmehr **§ 19a Abs. 2 Nr. 4a GWB** missbräuchliches Verhalten von Unternehmen mit überragender marktübergreifender Bedeutung durch die Verarbeitung wettbewerbsrelevanter Daten. Als ein solches Verhalten gilt es danach insbesondere, wenn das Unternehmen die Nutzung von Diensten davon abhängig macht, dass Nutzer der Verarbeitung von Daten aus anderen Diensten des Unternehmens oder eines Drittanbieters zustimmen, ohne ihnen eine ausreichende Wahlmöglichkeit zum Umstand, Zweck und Modalitäten der Verarbeitung einzuräumen. Das Bundeskartellamt (BKartA) kann ein solches Verhalten untersagen. Für Rechtsbehelfe gegen eine entsprechende Verfügung ist nach § 73 Abs. 5 Nr. 1 GWB unmittelbar der Bundesgerichtshof zuständig; der sonst übliche Weg über die Vorinstanz des OLG Düsseldorf (wie im Fall des Verfahrens zum Marktmissbrauch von Facebook, dazu TB 2020 Rn. 37 ff. und unten Rn. 45 ff.) entfällt. Die EU-Kommission plant mit dem Digital Market Act (DMA, Art. 5 lit. a des Entwurfs, oben Rn. 9) eine Regelung, die § 19a Abs. 2 Nr. 4a GWB weitgehend entspricht. Spätestens dann wird es möglich sein, die datenschutzrechtlichen Schutzziele auch mithilfe des Wettbewerbsrechts europaweit durchzusetzen. Im Sinne eines effektiven Datenschutzes ist dies nachdrücklich zu begrüßen.

25 Ein weiterer Baustein dieser Entwicklung ist das Gesetz zur Neuregelung von Verbraucherverträgen über digitale Produkte. Es setzt die sogenannte Digitale Inhalterichtlinie der EU vom 19. Mai 2019[11] um. Die **§§ 312 Abs. 1a bzw. 327 Abs. 3 BGB** stellen nunmehr klar, dass die Preisgabe personenbezogener Daten als Gegenleistung für eine Ware oder Dienstleistung wie ein finanzielles Entgelt zu behandeln ist. Das führt außerdem dazu, dass entsprechende Streitfragen als verbraucherschutzrechtlich zu qualifizieren und daher auch durch die entsprechenden Verbände aufgreifbar sind. Die Anbieter müssen die Verbindung von Leistung und personenbezogenen Daten nun eindeutig bezeichnen und den Kunden auch unter vertrags- bzw. verbraucher-, nicht nur unter datenschutzrechtlichen Gesichtspunkten ausdrücklich zur Einwilligung in die Verarbeitung seiner personenbezogenen Daten auffordern.

26 Erwähnt sei außerdem noch, dass der Bund im Zuge einer Novellierung des **BPersVG** (§ 69 S. 2) und des **BetrVG** (§ 79a S. 2) klargestellt hat, dass Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften (Art. 4 Nr. 7 DSGVO) für die Datenverarbeitung des Personal- bzw. Betriebsrats nicht dieser selbst, sondern die jeweilige Dienststelle ist. Dies entspricht meiner schon zuvor vertretenen Auffassung (TB 2019 Rn. 203). Die Klarstellung ist in jedem Falle begrüßenswert. Unberührt davon bleiben selbstverständlich die eigenständigen Rechte und Pflichten der Mitarbeitervertretungen, die der Verantwortliche unbeschadet seiner datenschutzrechtlichen Gesamtverantwortung zu respektieren hat.

[11] Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, AmtsBl (EU) L 136/1 vom 22.5.2019.

27 Der Vollständigkeit halber sei schließlich noch auf eine „Leerstelle“ hingewiesen, die der Bund im Berichtsjahr hinterlassen hat: Bis zum 17. Dezember 2021 hätte er nach deren Art. 26 Abs. 1 die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (**Whistleblower-Richtlinie**, s. dazu TB 2019 Rn. 26 f.) in deutsches Recht umsetzen müssen. Dazu ist es bislang nicht gekommen. Das ist bedauerlich, weil die Richtlinie dazu beitragen soll, gerade auch Verstöße gegen den Schutz personenbezogener Daten aufzudecken und Hinweisgeber zu schützen. Als interne „Meldestelle“ für ein geeignetes internes Hinweisgebersystem können die Verantwortlichen auch den internen Datenschutzbeauftragten benennen. Die an der neuen Bundesregierung beteiligte Parteien haben im Koalitionsvertrag vorgesehen, die entsprechenden Vorgaben nun „rechtssicher und praktikabel“ in deutsches Recht zu transformieren.

cc) Bundesländer

28 Die Bundesländer haben im Berichtsjahr keine nennenswerten Gesetzesänderungen mit Bezug zum Mediendatenschutz veranlasst. Klarstellungsbedarf besteht allerdings, wie oben (Rn. 20 f.) bereits angemerkt, zur Zuständigkeit der Datenschutzaufsicht auch zur Durchsetzung der aus den §§ 19 bis 25 TTDSG folgenden Vorgaben zum Schutz der Privatsphäre. Im Verhältnis zu den Rundfunkanstalten und ihren Beteiligungsunternehmen in meinem Zuständigkeitsbereich ist dies konsequenterweise der Rundfunkdatenschutzbeauftragte. Alle Bundesländer sollten sich möglichst zügig auf eine einheitliche – wenn auch landesspezifisch unterschiedlich umzusetzende – Regelung verständigen.

b Datenschutzrelevante Entwicklungen

aa) Internationaler Datenverkehr

29 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 oder Amazon (das mit AWS das weltweit größte Cloud-System anbietet) oder der Nutzung von Drittplattformen von Konzernen wie Google (YouTube) oder Meta (Facebook, WhatsApp, Instagram) verbunden (dazu auch unten Rn. 113 ff.). Nach Art. 44 S. 1 DSGVO ist sie allerdings grundsätzlich nur 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. Wie aus Art. 44 S. 2 DSGVO hervorgeht, ist genau dies die Absicht: Danach sind alle Bestimmungen (des entsprechenden Abschnitts) anzuwenden, um sicherzustellen, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

30 Indessen wären die Verantwortlichen mit einer Prüfung, ob Drittstaaten ein der DSGVO entsprechendes Schutzniveau vorsehen, im Zweifel überfordert; zudem kann auf diesem Weg das von der DSGVO angestrebte einheitliche Verständnis aller datenschutzrechtlichen Rahmenbedingungen kaum herbeigeführt werden. Daher sieht Art. 45 DSGVO eine ent-

sprechende 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.

31 Bislang hat die Kommission gut ein Dutzend Angemessenheitsentscheidungen veröffentlicht[12]. Mit Abstand die größte Bedeutung hat insoweit das Verhältnis zu den **USA**. Nachdem der EuGH im Juli 2020[13] mit seinem Schrems II-Urteil das Abkommen zum US-Privacy-Shield für unwirksam erklärt hatte (dazu TB 2020 Rn. 23), ist ein solcher allerdings nicht mehr vorhanden. Seither ist die Inanspruchnahme von Dienstleistungen US-amerikanischer Konzerne, die – wie im Falle von Büroanwendungen, der Nutzung von Kollaborationswerkzeugen sowie Clouds und Drittplattformen – mit einer Verarbeitung personenbezogener Daten verbunden sind oder sie sogar zum Gegenstand haben, nur noch unter engen Voraussetzungen zulässig. Denn der EuGH betrachtet das Datenschutzniveau in den USA als dem der DSGVO nicht adäquat. Ursächlich dafür ist unter anderem der im März 2018 in Kraft getretene sog. CLOUD- (**C**larifiying **L**awful **O**verseas **U**sing of **D**ata-) Act. Denn dessen Vorgaben verpflichten US-amerikanische Unternehmen, den dortigen Behörden einen Zugriff auf die von ihnen verarbeiteten Daten unabhängig davon zu ermöglichen, ob es sich um eigene oder im Auftrag Dritter verarbeitete Daten handelt und wo die Verarbeitung stattfindet.

32 Vergleichsweise unproblematisch stellt sich eine Datenübermittlung hingegen im Verhältnis zum bisherigen EU-Mitglied **Großbritannien** dar. Auf der Grundlage des Angemessenheitsbeschlusses der EU-Kommission vom 28. Juni 2021[14] ist sie in dieses Drittland weiterhin in gleicher Weise möglich wie innerhalb des Geltungsbereichs der DSGVO.

33 Soweit ein derartiger Angemessenheitsbeschluss nicht vorliegt, macht Art. 46 DSGVO die Übermittlung personenbezogener Daten an ein Drittland von zwei Bedingungen abhängig: Zum einen müssen anderweitige geeignete Garantien die Standards der DSGVO absichern, und zum anderen müssen den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Dazu können unter anderem von der Kommission verabschiedete **Standardvertragsklauseln** gehören, Art. 46 Abs. 2 DSGVO. Die bislang geltenden Klauseln hat die EU-Kommission mit Blick auf die Anforderungen der DSGVO sowie die technische Entwicklung weitgehend überarbeitet und in der Fassung vom 4. Juni 2021 neu veröffentlicht[15]. Seit dem 27. September 2021 sind sie im Sinne eines Mindeststandards verbindlich. Wie bisher ersetzen sie also keine eigenständige Prüfung des jeweiligen Verantwortlichen, ob einzelfallbezogen noch weitergehender Regelungs- bzw. Absicherungsbedarf besteht (Erwägungsgrund 3 des Durchführungsbeschlusses).

---

12 Europäische Kommission. Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de [Stand: 25.02.2022]

13 EuGH, Urteil vom 16. Juli 2020 – C 311/18 – (Schrems II).

14 Durchführungsverordnung (EU) 2021/1772 der Kommission vom 28. Juni 2021, AmtsBl (EU) L 360/1 vom 11.10.2021.

15 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021, AmtsBl (EU) L 199/31 vom 7.6.2021.

34 Die Übermittlung personenbezogener Daten in einen Drittstaat ohne Angemessenheitsbeschluss setzt also drei Maßnahmen des Verantwortlichen voraus: (1) Er muss sich gründlich mit allen Risiken des Datentransfers befassen und die für sie jeweils maßgeblichen Gesichtspunkte bewerten. (2) Er muss wirksame und durchsetzbare vertragliche Absprachen über alle erforderlichen technischen und organisatorischen Maßnahmen herbeiführen. (3) Und schließlich muss er die Gründe für seine Entscheidung, trotz der verbleibenden Risiken den entsprechenden Dienst zu nutzen, gem. Art. 5 Abs. 2 DSGVO dokumentieren. Unberührt bleibt außerdem seine Verpflichtung, die betroffenen Personen nach Art. 13 bzw. 14 Abs. 1 lit. f DSGVO über die beabsichtigte Übermittlung ihrer personenbezogenen Daten in ein Drittland zu informieren.

35 Das für die verbindliche Einbeziehung der Standardvertragsklauseln in das jeweilige Vertragsverhältnis erforderliche Einverständnis ist den US-amerikanischen Großkonzernen freilich allenfalls unter größtem Aufwand und mit entsprechendem Nachdruck abzuringen. Ausnahmen von diesem Erfordernis sieht Art. 49 DSGVO indessen lediglich für bestimmte Fälle und unter engen Voraussetzungen vor. Nötigenfalls bleibt daher nur, auf einen Vertragspartner (bzw. dessen Dienstleistungen) auszuweichen, der ein der DSGVO entsprechendes Datenschutzniveau garantieren kann - oder äußerstenfalls auf das entsprechende Vorhaben vollständig zu verzichten, solange es nicht DSGVO-konform durchführbar ist.

36 Die staatlichen Aufsichtsbehörden haben im Berichtsjahr begonnen, ausgewählte Verantwortliche in ihrem Zuständigkeitsbereich mithilfe eines gemeinsamen Fragekatalogs um Auskunft zu den Modalitäten etwaiger Datenübermittlung in Drittländer, insbesondere die USA, sowie die Umsetzung der aus dem Schrems II-Urteil des EuGH folgenden Vorgaben zu bitten. Dabei soll es unter anderem um den Einsatz von Dienstleistungen zum E-Mail-Versand, zum Hosting von Internetseiten, zur Verwaltung von Daten in Bewerbungsverfahren, um den konzerninternen Austausch von Kunden- und Beschäftigtendaten sowie um das Webtracking gehen[16].

bb) Rechtsprechung auf europäischer Ebene

37 Auf den hohen Stellenwert, den der **Europäische Gerichtshof** dem Grundrecht auf Datenschutz beimisst, habe ich bereits früher hingewiesen[17]. Insbesondere die Konsequenzen seiner Entscheidung zum sogenannten Privacy-Shield-Abkommen (Schrems II)[18] sind weitreichend. Diese hat auch für die Verantwortlichen meines Zuständigkeitsbereichs unmittelbaren Prüfungs- und ggf. Handlungsbedarf ausgelöst, soweit sie Anwendungen US-amerikanischer Hersteller einsetzen, die personenbezogene Daten Dritter in die USA übermitteln. Zwar können sie nun auf die aktualisierten Standardvertragsklauseln der EU-Kommission zurückgreifen (oben Rn. 33). Allerdings erfordert dies entsprechende (nachträgliche) Abreden mit dem jeweiligen Vertragspartner. Abgesehen davon müssen sie je

[16] S. bspw.: Der Hamburgische Datenschutzbeauftragte für Datenschutz und Informationsfreiheit. Koordinierte Prüfung internationaler Datentransfers, https://datenschutz-hamburg.de/pages/fragebogenaktion/ [Stand: 25.02.2022]

[17] TB 2019 Rn. 48 ff.; TB 2020 Rn. 26 ff.

[18] S. schon oben Rn. 31

nach Sachlage darüberhinausgehende zusätzliche Maßnahmen vorsehen, um die Einhaltung des erforderlichen Schutzniveaus wirksam zu gewährleisten und durchzusetzen. Und sie haben zudem fortlaufend zu überprüfen, ob die vertraglich vereinbarten Maßnahmen effektiv umgesetzt werden und wirken. Anderenfalls ist eine Datenübermittlung in das Drittland – insbes. die USA – unzulässig, und die zuständige Aufsichtsbehörde – in diesem Fall also der Rundfunkdatenschutzbeauftragte - ist gehalten, sie gegebenenfalls auch zu unterbinden[19].

38 Mit damit verbundenen aufsichtsrechtlichen Fragen hat sich der EuGH in seinem **Urteil vom 15. Juni 2021**[20] befasst, in dem es einmal mehr um Facebook ging. Auslöser war, dass die Belgische Datenschutzaufsichtsbehörde Facebook aufgefordert hatte, es zu unterlassen, mittels Cookies, Social Plugins und Pixeln personenbezogene Daten der Internetnutzer im belgischen Hoheitsgebiet zu verarbeiten. Da sich die Hauptniederlassung von Facebook Europa in Dublin befindet, ist für das Unternehmen eigentlich jedoch die Irische Aufsichtsbehörde federführend zuständig. Sie war allerdings anhaltend untätig geblieben. Der EuGH stellte fest, dass eine Aufsichtsbehörde eine entsprechende Maßnahme grundsätzlich auch dann veranlassen darf, wenn es sich um eine grenzüberschreitende Datenverarbeitung handelt und sie nicht „die zuständige federführende Aufsichtsbehörde" im Sinne der Kohärenzvorschriften nach Artt. 60 ff. DSGVO ist. Allerdings muss sie zuvor die dort vorgesehenen Verfahren der Zusammenarbeit und Kohärenz eingehalten, also die federführende Behörde förmlich einbezogen haben. Unter dieser Voraussetzung komme es auch nicht darauf an, ob der für die grenzüberschreitende Datenverarbeitung Verantwortliche im Hoheitsgebiet des Mitgliedstaats der betreffenden Aufsichtsbehörde eine (Haupt-) Niederlassung habe.

39 Mehrfach hat sich im Berichtsjahr auch der **Europäische Gerichtshof für Menschenrechte** (EGMR) mit datenschutzrechtlich relevanten Fragen befasst. Dabei ging es jeweils um das Verhältnis zwischen dem Schutz des Persönlichkeitsrechts bzw. dem Recht auf Datenschutz zu dem in Art 10 EMRK geschützten Recht auf freie Berichterstattung. So bejahte er in einem **Urteil vom 22. Juni 2021**[21] das „Recht auf Vergessen" in Bezug auf ein Online-Zeitungsarchiv. Konkret ging es um den Namen eines an einem tödlichen Unfall beteiligten Autofahrers, den die (belgische) Zeitung in einem Artikel vollständig veröffentlicht hatte, den sie dann unverändert in ihr Onlinearchiv aufnahm. Der Betroffene hatte verlangt, den Artikel nachträglich zu anonymisieren. Der EGMR hielt dies für verhältnismäßig, weil der Betroffene keine Person des öffentlichen Lebens gewesen sei und seine Strafe verbüßt habe. Er müsse es deshalb nicht hinnehmen, dass bei einer Internetsuche nach seinem Namen auf Dauer unmittelbar der Artikel über den damaligen Unfall angezeigt werde. Der Artikel könne auch mit unkenntlich gemachtem Namen im Archiv gelesen werden.

40 Zugleich stellte der EGMR allerdings auch fest, dass die Medien nicht verpflichtet seien, ihre (öffentlich zugängliche) Archive laufend daraufhin zu überprüfen, ob die Veröffentlichung noch zulässig sei. Dies und eine Abwägung der dabei jeweils betroffenen Belange sei

---

19 EuGH, Urteil vom 16. Juli 2020 – C-311/18 – (Schrems II) Rn. 134 f. S. dazu auch unten 115.

20 EuGH, Urteil vom 15. Juni 2021 – C-645/19 -, Facebook Ireland Limited, Facebook INC, Facebook Belgium BVBA vs. Gegevensbeschermingsautoriteit

21 EGMR, Urteil vom 22. Juni 2021 – 57292/16 -, Hurbain vs. Belgien

vielmehr nur auf entsprechendes ausdrückliches Verlangen einer betroffenen Person erforderlich (s. dazu bereits die ausführlichen Hinweise auf die Rechtsprechung des BVerfG im TB 2019 Rn. 62 ff.).

41 Das **Urteil vom 25. November 2021**[22] betrifft ebenfalls das „Recht auf Vergessen". Eine italienische Zeitung hatte über eine Messerstecherei in einem Restaurant berichtet und dabei dessen in die Auseinandersetzung verwickelte Inhaber namentlich genannt. Die Betroffenen verlangten zwei Jahre später von der Zeitung vergeblich, den Zugang zu dem Artikel im Internet durch geeignete Maßnahmen („De-Indexierung") zu erschweren bzw. zu unterbinden. Mit ihrer dahingehenden Klage waren sie erfolgreich. Gegen die letztinstanzliche Entscheidung wehrte sich die Zeitung vergeblich vor dem EGMR, der seinem Urteil das hier maßgebliche italienische Datenschutzrecht im Lichte der europäischen Regelungen, insbesondere der DSGVO (Art. 17 Abs. 1), zugrunde legte. Dieses sei so auszulegen, dass das Recht der Zeitung auf eine namentliche Berichterstattung angesichts der konkreten Umstände des Falles im Laufe der Zeit hinter dem Anspruch der Betroffenen auf Schutz ihrer Persönlichkeit zurücktreten müsse. Dies gelte umso mehr, als die Zeitung nicht verpflichtet worden sei, den Artikel insgesamt dauerhaft zu sperren.

42 In seinem **Urteil vom 7. Dezember 2021**[23] schließlich hatte sich der EGMR mit einem Rechtsstreit zu befassen, in dem ein FPÖ-Politiker von der österreichischen Zeitung „Der Standard" verlangte, ihm die personenbezogenen Daten mehrerer Onlinenutzer offenzulegen, gegen deren Kommentare im Onlineangebot der Zeitung er sich gerichtlich zur Wehr setzen wollte. Der EGMR stellte fest, dass die Zeitung dies nicht unter Berufung auf den Quellen- bzw. Informantenschutz verweigern könne. Denn die Kommentare seien an die Öffentlichkeit und nicht an die Zeitung gerichtet. Wohl aber sei jedenfalls angesichts der konkreten Ausgestaltung des vom „Standard" angebotenen Onlineportals mittelbar dessen Rolle als Forum der öffentlichen Meinungsbildung betroffen. Sie sei gefährdet, wenn die Zeitung verpflichtet werden könne, die personenbezogenen Daten ihrer Nutzer auch dann offenzulegen, wenn es – wie hier – um keine offenkundig gravierenden, insbesondere strafbaren Persönlichkeitsrechtsverletzungen gehe. Daher verstieß die gegenteilige Entscheidung des höchsten österreichischen Gerichts nach (mehrheitlicher[24]) Auffassung des EGMR gegen Art. 10 EMRK.

43 Schließlich sei noch erwähnt, dass der EGMR im Januar 2021 eine schon im Jahr 2017 eingereichte Beschwerde der Organisation „Reporter ohne Grenzen"[25] gegen die anlasslose Fernmeldeüberwachung des BND zur Entscheidung angenommen hat[26]. Nach Auffassung

---

22 EGMR, Urteil vom 25. November 2021 – 77419/16 -, Biancardi vs. Italien

23 EGMR, Urteil vom 7. Dezember 2021 – 39378/15 -, Standard Verlagsgesellschaft mbH vs. Österreich

24 In einer „Dissenting Opinion" sprach sich der deutsche Richter Eicke gegen die Ausweitung des Schutzbereichs von Art. 10 EGMR auf Serviceprovider aus; eher als solcher (und weniger als Medienanbieter) sei nämlich in Bezug auf die Kommentarplattform auch „Der Standard" zu qualifizieren. Anderenfalls sei zu befürchten, dass der Betroffenenschutz nicht hinreichend gewährleistet werden könne.

25 Reporter ohne Grenzen. Beschwerde nach Artikel 34 EMRK. https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Dokumente/171128_EGMR-Schriftsatz_ROG.PDF [Stand: 25.02.2022]

26 Reporter ohne Grenzen (2021, 11.01.). Etappensieg für Beschwerde gegen BND [Pressemitteilung]. https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/egmr-laesst-beschwerde-gegen-bnd-zu [Stand: 25.02.2022]

der Organisation verletzt diese auf das sogenannte G10-Gesetz gestützte Praxis insbesondere die in Art. 10 EMRK geschützte Meinungs- und Informationsfreiheit, weil sie das Redaktionsgeheimnis und den Informantenschutz unterlaufe. Vor dem Bundesverwaltungsgericht (BVerwG) waren die Organisation bzw. einzelne Kläger gescheitert, weil sie nach Auffassung des BVerwG nicht hinreichend konkret hätten nachweisen können, dass sie von der Praxis individuell betroffen seien. Eine dagegen gerichtete Verfassungsbeschwerde nahm das BVerfG, anders als nun der EGMR, nicht zur Entscheidung an.

cc) Rechtsprechung in Deutschland

44 Aus der deutschen Rechtsprechung sei hier nur auf einige besonders bedeutsame Verfahren mit Bezug zum Mediendatenschutz hingewiesen. Zwei von ihnen betreffen Facebook:

45 Wie berichtet (TB 2019 Rn. 70), hatte das BKartA am 6. Februar 2019 Facebook untersagt, auf der Grundlage seiner Nutzungsbedingungen nutzer- und gerätebezogene Daten, die bei der Nutzung sonstiger Facebook-Produkte, insbesondere von WhatsApp, mobiler Apps und dem Besuch dritter Webseiten anfallen, mit den unmittelbar auf Facebook erhobenen personenbezogenen Daten seiner Nutzer zusammenzuführen. Die formal erteilte Einwilligung der Nutzer mit dieser Praxis sei angesichts der Marktmacht von Facebook nicht freiwillig im Sinne des Art. 7 DSGVO. Der darin begründete Verstoß der Datenverarbeitung gegen Art. 6 DSGVO sei zugleich nach § 19 Abs. 1 GWB als Missbrauch einer marktbeherrschenden Stellung zu qualifizieren. Einem daraufhin von Facebook gestellten Antrag auf Aussetzung des Vollzugs der entsprechenden Untersagungsverfügung gab das OLG Düsseldorf wegen erheblicher Zweifel an dessen Rechtmäßigkeit statt (TB 2019 Rn. 71). Auf die dagegen erhobene Beschwerde verwarf der BGH jedoch den Beschluss des OLG Düsseldorf und wies den Eilantrag von Facebook zurück (TB 2020 Rn. 37 ff.).

46 In dem jetzt durchzuführenden Hauptsachverfahren legte inzwischen das **OLG Düsseldorf** – wie zu erwarten war (TB 2020 Rn. 39) - mit **Beschluss vom 24.3.2021**[27] dem EuGH sieben Fragen zur Auslegung der DSGVO vor, die es als entscheidungserheblich ansieht. Insbesondere soll der EuGH klären, ob es mit den Zuständigkeitsregelungen der Artt. 51 ff. DSGVO vereinbar ist, dass eine nationale Wettbewerbsbehörde wie das BKartA einen (vermeintlichen) Verstoß gegen datenschutzrechtliche Vorschriften sanktioniert. Ferner hält es das OLG Düsseldorf für klärungsbedürftig, ob das BKartA sich inhaltlich mit Fragen der Anwendung bzw. Umsetzung der DSGVO befassen darf. Und es wirft die Frage auf, ob Facebook als marktbeherrschendes Unternehmen von seinen Nutzern überhaupt wirksam eine Einwilligung einholen könne.

47 Ein noch längerer Verfahrensvorlauf hat zu dem **Urteil des OVG Schleswig-Holstein vom 25.11.2021**[28] geführt. Fast auf den Tag genau zehn Jahre zuvor hatte die Landesdatenschutzbehörde Schleswig-Holstein der Wirtschaftsakademie, einer Bildungseinrichtung mit Sitz in Schleswig-Holstein, untersagt, einen Nutzer-Account in Gestalt einer sogenannten Fanpage bei Facebook zu betreiben. Dagegen klagte die Einrichtung mit Erfolg vor dem

[27] OLG Düsseldorf, Beschluss vom 24. März 2021 – Kart 2/19 (V) -.
[28] OLG Schleswig-Holstein, Urteil vom 25. November 2021 – 4 LB 20/13 -.

Verwaltungs- wie auch Oberverwaltungsgericht. Im Revisionsverfahren legte das BVerwG dem EuGH die Frage zur Vorabentscheidung vor, ob der Betreiber einer Fanpage gemeinsam mit Facebook verantwortlich für die damit verbundene Datenverarbeitung sei. Der EuGH bejahte dies mit seinem Urteil vom 5. Juni 2018 grundsätzlich. Daraufhin hob das BVerwG am 11. September 2019 das Berufungsurteil auf und verwies die Sache zur erneuten Prüfung und Entscheidung an das OVG Schleswig-Holstein zurück (TB 2019 Rn. 68 f.).

48 Dieses stellte nun fest, dass der Betreiber einer Fanpage jedenfalls für die Verarbeitung personenbezogener Daten der bei Facebook registrierten Nutzer mit verantwortlich sei, die in die von Facebook zur Verfügung gestellte Insight-Statistik für diese Fanpage einfließen; hingegen sei Facebook allein verantwortlich für die weitere Verwendung dieser Daten für Profile und Werbezwecke. Dementsprechend erstrecke sich die Mitverantwortung des Fanpage-Betreibers auch auf die mit der Datenverarbeitung verbundenen Informationspflichten. Im vorliegenden Fall sei die konkrete Datenverarbeitung durch Facebook weder durch einen gesetzlichen Erlaubnistatbestand, der das ansonsten geltende Verarbeitungsverbot aufhebt, noch durch eine wirksam erteilte Einwilligung gerechtfertigt. Die unzulässige Verwendung ihrer Daten zur Anfertigung der Insights wie auch die unzureichende Information darüber verletzten daher das Recht auf informationelle Selbstbestimmung der Facebooknutzer, namentlich der zahlreich betroffenen Jugendlichen. Denn sie könnten überhaupt nicht nachvollziehen, welche ihrer personenbezogenen Daten in welcher Form ggf. Dritten zur Verfügung gestellt werden. Dies sei ein schwerwiegender Datenschutzverstoß, der die schleswig-holsteinische Datenschutzbehörde zurecht zur Anordnung veranlasst habe, die Fanpage abzuschalten (s. zu diesem Thema auch unten Rn. 113 ff.).

49 Auch das **Bundesarbeitsgericht** (BAG) hat in einem bei ihm anhängigen Verfahren zwei Fragen vorab dem EuGH zur Entscheidung vorgelegt[29]. Konkret geht es um die Abberufung eines betrieblichen Datenschutzbeauftragten, der zugleich Betriebsratsvorsitzender war. Das Unternehmen hatte sich auf den Standpunkt gestellt, dass nach Inkrafttreten der DSGVO eine solche Doppelfunktion mit den Vorgaben zur Unabhängigkeit des internen Datenschutzbeauftragten nach Art. 37 DSGVO unvereinbar sei. Allerdings lässt § 6 Abs. 4 BDSG die Abberufung des internen Datenschutzbeauftragten nur unter den Voraussetzungen einer außerordentlichen Kündigung entsprechend § 626 BGB zu. Das deutsche Recht ist damit restriktiver als Art. 38 Abs. 3 DSGVO. Die Zulässigkeit einer solchen Abweichung muss der EuGHG feststellen. Das BAG hält eine Abberufung nach § 626 BGB an und für sich nicht für gerechtfertigt, hat aber den EuGH vorsorglich auch um die Beantwortung der Frage gebeten, ob die genannte Doppelfunktion einen Interessenkonflikt iSv. Art. 38 Abs. 6 S. 2 DSGVO begründen kann. Mittelbar geht es dabei auch um die Reichweite der Kontrollbefugnisse des internen Datenschutzbeauftragten gegenüber dem Betriebs- bzw. Personalrat (s. dazu schon TB 2019 Rn. 204 ff.).

50 In einer weiteren Entscheidung vom selben Tag hat der 2. Senat des BAG sich mit dem Anspruch auf Überlassung einer Datenkopie nach Art. 15 Abs. 3 DSGVO im Beschäftigungsverhältnis befasst[30]. Der Kläger hatte die Kopie der personenbezogenen Daten gefordert, die Gegenstand einer ihm erteilten Auskunft waren. Außerdem verlangte er aber auch Ko-

[29] BAG, Beschluss vom 27. April 2021 – 9 AZR 383/19 -
[30] BAG, Urteil vom 27. April 2021 – 2 AZR 342/20 -

pien des gesamten E-Mail-Verkehrs des Arbeitgebers, in dem er namentlich genannt worden war. Die Vorinstanzen hatten seiner Klage im ersten Punkt stattgegeben und sie im übrigen abgewiesen. Dem schloss sich das BAG an. Allerdings ließ es – leider - offen, ob sich der Anspruch auf eine Kopie nach Art. 15 Abs. 3 DSGVO tatsächlich auch auf interne E-Mail-Korrespondenz oder sonstige interne Unterlagen beziehen kann (s. meine Position dazu TB 2019 Rn. 154 ff.). Jedenfalls sei eine bloß abstrakte Nennung der Kategorien von E-Mails, von denen eine Kopie überlassen werden solle, mangels hinreichender Bestimmtheit nicht vollstreckbar und daher prozessual unzulässig.

51 Ausgesprochen weit interpretiert der **Bundesgerichtshof**[31] das Recht auf Auskunft nach Art. 15 DSGVO. Ein Versicherungsnehmer hatte im Zusammenhang mit einer Rückzahlungsforderung gegenüber seiner Versicherung Auskunft über alle dort zu seiner Person gespeicherten Daten verlangt. Unter anderem bezog er sich dabei auf seine mit ihr geführte Korrespondenz, die vollständigen Daten seines Prämienkontos und sämtliche Telefon-, Gesprächs- und Bewertungsvermerke. Der BGH hielt es für unschädlich, dass sich das Auskunftsbegehren teilweise auf Daten bezog, die dem Antragsteller bekannt waren. Auch interne Vermerke seien grundsätzlich nicht ausgenommen, denn eine dahingehende Einschränkung lasse sich weder aus dem Wortlaut noch aus Sinn und Zweck des Art. 15 DSGVO ableiten. Da der BGH sich auf die Rechtsprechung des EuGH berief, hielt er es auch nicht für erforderlich, diesem die Streitfrage zur Vorabentscheidung vorzulegen. Generell hält er den Auskunftsanspruch nur dort für ausgeschlossen, wo sich ein Grund für dessen Ablehnung unmittelbar aus der DSGVO herleiten lässt.

52 Erwähnenswert ist schließlich noch ein Beschluss des **OVG Rheinland-Pfalz**[32], in dem es um die Reichweite des Begriffs der „Datenverarbeitung zu journalistischen Zwecken“ ging, an den das sogenannte „Medienprivileg“ anknüpft (dazu ausführlich TB 2019 Rn. 6 ff.). Schon aus Erwägungsgrund 153 DSGVO ergibt sich, dass er sehr weit auszulegen ist, und der EuGH hat dies ausdrücklich bekräftigt (s. bereits TB 2019 Rn. 49). Er umfasst sowohl die Datenverarbeitung zum Gegenstand bzw. Inhalt der Berichterstattung selbst wie auch die Datenverarbeitung zur Produktion, Verarbeitung, Gestaltung, Platzierung und Verbreitung der betreffenden Informationen. Ob die Datenverarbeitung aber tatsächlich „journalistischen Zwecken“ dient, ist gleichwohl nicht immer ohne weiteres zu beantworten. Einigkeit besteht darüber, dass dies nur dann zu bejahen ist, wenn sie zur öffentlichen Meinungsbildung beitragen soll. Angesichts der unüberschaubaren Vielfalt elektronischer Kommunikationsformen und -beteiligten sind die Grenzen zwischen Individual- und Massenkommunikation einerseits sowie zwischen Äußerungen zur öffentlichen Meinungsbildung und der bloßen Kundgabe individueller (Kommentar o.ä.) oder institutioneller (Öffentlichkeitsarbeit etc.) Meinungen „in eigener Sache“ freilich fließend.

53 Genau diese Abgrenzungsfrage stellte sich in dem vom OVG Koblenz zu beurteilenden Sachverhalt: Dort hatte der Kläger gem. § 20 MStV eine Gegendarstellung zu einem Beitrag verlangt, den eine Anwaltskanzlei in einem Blog auf ihrer Homepage veröffentlicht hatte. Dafür hätte es sich bei dem Blog bzw. der Homepage allerdings um ein „Telemedium mit journalistisch-redaktionell gestalteten Angeboten“ handeln müssen. Die dafür erfor-

[31] BGH, Urteil vom 15. Juni 2021 – VI ZR 576/19 -.
[32] OVG Rheinland-Pfalz, Beschluss vom 12. April 2021 – 4 W 108/21 -.

derliche publizistische Zielsetzung vermisste das OVG Koblenz jedoch. Die dort abrufbaren Beiträge seien nicht als (Fach-)Journalismus zu qualifizieren, sondern dienten lediglich der Selbstdarstellung, also der Öffentlichkeitsarbeit bzw. dem Marketing der Kanzlei.

dd) Datenschutzprobleme

54 Das Berichtsjahr war geprägt von wiederholten Warnungen des BSI vor zunehmenden **Cyberangriffen** auf die IT-Infrastrukturen und Datenbestände, und sich häufenden gravierenden Vorfällen dieser Art. Einmal mehr waren davon unter anderem auch die großen sogenannten Sozialen Netzwerke wie Facebook, LinkedIn[33] oder Clubhouse[34] betroffen, mit der Folge, dass Millionen von Nutzerdaten öffentlich zugänglich waren bzw. auf Hacker-Foren zum Kauf angeboten wurden. Erhöht wird die Gefahr solcher Angriffe durch den von der Corona-Pandemie ausgelösten Schub zur Digitalisierung und Flexibilisierung der Arbeitswelt. Diese an und für sich positive (und längst überfällige) Entwicklung geht leider mit erhöhten Risiken für Datenschutz und Datensicherheit einher (dazu bereits TB 2020 Rn. 40 f.). Erfreulicherweise sind mir im Berichtsjahr keine größeren Probleme dieser Art in meinem Zuständigkeitsbereich gemeldet worden.

55 Der **Medienbereich** als solcher ist freilich mitnichten vor ihnen gefeit. Das hat sich dafür an anderer Stelle mehrfach erwiesen: Sowohl die Funke Mediengruppe bzw. die von ihr herausgegebene Zeitung WAZ (Jahreswechsel 2020/2021)[35] wie auch die Verlagsgruppe Madsack (März 2021)[36], Radio Energy Hamburg (Mai 2021)[37] oder die TAZ (Dezember 2021)[38] waren Opfer solcher kriminellen Attacken[39]. Während etwa die WAZ und Regionalzeitungen der Madsack-Gruppe daraufhin über längere Zeit nur mit einer Notausgabe erschienen oder der Radiosender Energy Hamburg nur ein Ersatzprogramm senden konnte, waren im Falle der TAZ die E-Mail-Adressen und weitere Daten der Kunden ihres Digitalabonnements nicht hinreichend gesichert gewesen.

---

33 Rixecker, Kim (2021, 09. April). Nach Facebook kommt LinkedIn: Zweites großes Datenleck in nur einer Woche, t3n. https://t3n.de/news/linkedin-datenleck-leak-facebook-1371601 [Stand: 25.04.2022]

34 Bielawa, Helen (2021, 11. April). Nach Facebook- Linkedin-Leaks: Clubhouse-Nutzerdaten im Netz, t3n. https://t3n.de/news/clubhouse-daten-leak-1371735 [Stand: 25.04.2022]

35 Tyrock, Andreas (2021). Cyberangriff: Warum die WAZ nur als Notausgabe erscheint, WAZ. https://www.waz.de/region/rhein-und-ruhr/waz-erscheint-nur-als-notausgabe-freier-zugang-auf-waz-de-id231206840.html [Stand: 25.02.2022]

36 Herbstreuth, Mike; Constanze Kurz im Gespräch mit Isabelle Klein (2021, 26. April). Hackerangriff auf Verlag Madsack - "Unternehmen investieren zu wenig in IT-Sicherheit", Deutschlandfunk. https://www.deutschlandfunk.de/hackerangriff-auf-verlag-madsack-unternehmen-investieren-zu-100.html [Stand: 25.04.2022]

37 Radio Energy (2021). Hacker greifen Energy Hamburg an, https://www.energy.de/hamburg/on-air/hacker-greifen-energy-hamburg-an [Stand: 25.02.2022]

38 Krempl, Stefan (2022, 03.01.). Passwort geknackt: taz stellt Anzeige nach Datenleck beim Digitalabo, heise online. https://www.heise.de/news/Passwort-geknackt-taz-stellt-Anzeige-nach-Datenleck-beim-Digitalabo-6316937.html [Stand: 25.02.2022]

39 S. dazu etwa die ZDF-Dokumentation „Geld her oder Daten weg“ vom 10.2.2022.

56 Es bleibt zu hoffen, dass die technischen und organisatorischen Maßnahmen der Verantwortlichen in meinem Zuständigkeitsbereich durchweg dem höchsten Standard entsprechen und so die unvermeidbaren Risiken weitestmöglich reduzieren. Das gilt natürlich vor allem für die Rundfunkanstalten, die zwar nicht rechtlich (im Sinne des IT-Sicherheitsgesetzes), wohl aber faktisch zu den „kritischen Infrastrukturen" gehören, deren Funktionsfähigkeit gerade in Krisenzeiten zuverlässig gewährleistet sein muss (dazu ausführlich TB 2019 Rn 35 ff. sowie TB 2020 Rn. 13). Entsprechendes gilt, wenn auch aus anderen als publizistischen Gründen, für den Gemeinsamen Beitragsservice von ARD, ZDF und Deutschlandradio.

57 Dass zu den genannten „unvermeidbaren Risiken" auch quasi staatliche Aktionen gehören können, hat sich einmal mehr an der Enthüllung des sogenannten „**Pegasus-Projekts**" durch den Rechercheverbund von WDR, NDR und Süddeutscher Zeitung im Sommer 2021 gezeigt.[40] Es ist nach dem Produkt der israelischen NSO Group, eines weltweit führenden Herstellers von Überwachungssoftware, benannt. Während das Programm nach offiziellen Angaben grundsätzlich nur durch Behörden – etwa Geheimdienste, Polizei oder Militär - bei mutmaßlichen Kriminellen bzw. Terroristen eingesetzt werden soll, fand das Rechercheteam unter den potentiellen Zielpersonen auch mehr als 180 Journalistinnen und Journalisten. Dass ein solches Spähprogramm den Informantenschutz sowie das Redaktionsgeheimnis gefährden kann, liegt auf der Hand. Immerhin: Deutsche Behörden haben es offenbar bislang allenfalls in einer Basisversion und in streng begrenzten Einzelfällen eingesetzt; seine Anwendungsmöglichkeiten gehen ansonsten weit über das hinaus, was die deutschen Sicherheitsgesetze bisher zulassen.

58 Eine Spähsoftware anderer Art hat das Unternehmen Clearview AI entwickelt. Es wurde weltweit bekannt, als die New York Times im Januar 2020 enthüllte, dass es sein Produkt nicht nur an Strafverfolgungsbehörden in verschiedenen Ländern, sondern auch an private Unternehmen vertrieben hatte. Es handelt sich um eine **Gesichtserkennungssoftware**, für die das Unternehmen auf eine Datenbank mit angeblich mehr als 3 Milliarden Gesichtsbildern zurückgreift. Diese wiederum entsteht durch den Einsatz eines automatisierten „Image Scrapers", der das Internet durchsucht und alle als menschliches Gesicht erkannten Bilder sowie deren Metadaten (Bild- oder Webseitentitel, Geolokaldaten und Quelllink) erfasst und für unbestimmte Dauer speichert. Die von Max Schrems geführte NGO „noyb" und weitere Organisationen haben im Mai 2021 gegen diese Praktiken Beschwerde bei mehreren europäischen Datenschutzbehörden, darunter auch beim Hamburgischen Datenschutzbeauftragten, eingereicht.[41]

59 Ein (vermeintliches) Datenschutzproblem ganz eigener Art sei abschließend quasi unter der Rubrik „Vermischtes" erwähnt[42]: Am 17. Februar 2021 untersagte das Bezirksamt Ber-

[40] Obermaier, Frederik; Obermayer, Bastian (2021, 18. Juli). So lief die Projekt-Pegasus-Recherche, Süddeutsche Zeitung. https://www.sueddeutsche.de/projekte/artikel/politik/pegasus-project-so-lief-die-recherche-e571971 [Stand: 25.02.2022]

[41] Noyb (2021, 26. Mai). Europaweite Beschwerden gegen Clearview AI, https://noyb.eu/de/europaweite-beschwerden-gegen-clearview-ai [Stand: 25.02.2022]

[42] Frerichmann, Nora (2021, 18.02.). Eine Frage des Selbstzwecks, MDR – Das Altpapier. https://www.mdr.de/altpapier/das-altpapier-1872.html [Stand: 25.02.2022]

lin-Mitte **„tagesschau.de“** das **Streaming einer Pressekonferenz**, auf der es an diesem Tag gemeinsam mit dem Robert-Koch-Institut die Ergebnisse einer Studie über die Verbreitung des Coronavirus vorstellte. Es berief sich dabei bemerkenswerterweise auf den Datenschutz: Nach einer Rückmeldung der Berliner Datenschutzbeauftragten habe das Bezirksamt davon ausgehen müssen, dass die mit dem Livestream verbundene Übermittlung personenbezogener Daten in Bild und Ton nur mit Einwilligung aller Betroffenen zulässig sei; diese aber habe angesichts der kurzfristigen Anfrage der „Tagesschau“ nicht mehr rechtzeitig abgefragt und dokumentiert werden können.

60 Dass eine Liveübertragung durch ein Medium wie „tagesschau.de“ unzweifelhaft eine „Datenverarbeitung zu journalistischen Zwecken“ bedeutet, die den allgemeinen datenschutzrechtlichen Erlaubnistatbeständen nach Art. 6 DSGVO gar nicht unterliegt, war dem Bezirksamt (und der Berliner Landesdatenschutzbehörde) offenbar nicht geläufig. Der Datenschutz kann und darf einer ungehinderten Rundfunkberichterstattung grundsätzlich nicht entgegenstehen bzw. gegen sie in Stellung gebracht werden: das ist der Kern des sogenannten „Medienprivilegs“. Dazu besteht offenkundig noch erheblicher Aufklärungsbedarf. Dass die Verantwortlichen die Persönlichkeitsrechte der Betroffenen zu wahren haben, bleibt davon selbstverständlich unberührt, ist aber keine datenschutz(aufsichts)rechtliche Frage. Wie stets bei derartigen Anlässen wäre dafür keine förmliche Einwilligung jeder beteiligten Person erforderlich gewesen, sondern es hätte ein ausdrücklicher Hinweis auf die Übertragung im Livestream zu Beginn genügt.

61 Auf die zunehmend bedeutsamer werdenden verbraucherschutzrechtlichen Aspekte des Datenschutzes und die hilfreiche Rolle des BKartA in diesem Zusammenhang habe ich an anderer Stelle bereits hingewiesen (TB 2019 Rn. 41 f.). Dieses hat im Juli 2021 eine weitere verbraucherrechtliche Studie mit dem Titel **Sektoruntersuchung Mobile Apps**[43] veröffentlicht. Sie befasst sich eingehend unter anderem damit, ob und inwieweit die App-Store-Betreiber und App-Anbieter die für das Herunterladen, die Installation und die Nutzung solcher Apps maßgeblichen datenschutzrechtlichen Anforderungen einhalten bzw. umsetzen. Im Ergebnis erkennt das BKartA hier erhebliche Umsetzungsdefizite und entsprechenden Prüfungs- und Handlungs- bzw. Vollzugsbedarf sowohl auf der Aufsichtsebene wie auch in der privaten Rechtsdurchsetzung. Unter anderem spricht sich das BKartA mit Blick auf die supranationalen Tech-Konzerne für eine europäische Datenschutzbehörde aus, die – ähnlich wie das Netz der europäischen Wettbewerbsbehörden – große grenzüberschreitende Fälle behandeln könnte. Außerdem plädiert es dafür, App-Publisher zu sperren, die die daten- und verbraucherschutzrechtlichen Standards nicht umsetzen.

c Sonstiges

62 Nach Inkrafttreten der DSGVO im Mai 2016, spätestens aber bis zu deren unmittelbarem Wirksamwerden im Mai 2018 waren die nationalen Gesetze mit Datenschutzbezug den neuen Vorgaben anzupassen und die zahlreichen Regelungsaufträge umzusetzen. Dazu verabschiedete der Bundestag zwei umfangreiche Anpassungs-Artikelgesetze und novel-

[43] BKartA (2021, Juli): Sektoruntersuchung Mobile Apps [Bericht].

lierte vor allem das **BDSG** vollständig. Ausweislich der Gesetzesbegründung sollte die Neufassung spätestens drei Jahre nach Inkrafttreten, also bis Mai 2021, **evaluiert** werden.

63 Mit Schreiben vom 16. November 2020 übermittelte das für die Evaluation federführende Bundesministerium des Innern, für Bau und Heimat daraufhin den in der DSK zusammengeschlossenen staatlichen Datenschutzbehörden, öffentlichen Stellen des Bundes, Fachressorts der Länder sowie 88 Spitzenverbänden der Wirtschaft und weiteren Einrichtungen einen Fragebogen und gab ihnen Gelegenheit zur Stellungnahme. Die Mitglieder der RDSK gehörten hingegen bemerkenswerterweise nicht zu den weit mehr als 100 Adressaten. Erst Monate nach Ablauf der Stellungnahmefrist erfuhr ich über meinen Kontakt zur DSK-Vorsitzenden von dem Evaluationsverfahren. Das BMI, bei dem ich daraufhin die unterlassene Beteiligung beanstandete, hat mir zugesichert, in künftigen vergleichbaren Fällen auch die RDSK einzubeziehen.

64 Obwohl das BDSG für meine Aufsichtspraxis nur eingeschränkt relevant ist, hätte Anlass zu einer Stellungnahme mindestens mit Blick auf die Vorschrift des § 18 BDSG bestanden. Sie regelt die Einbeziehung der sogenannten „spezifischen Aufsichtsbehörden" in das Verfahren zur einheitlichen Umsetzung der DSGVO bisher nur unbefriedigend. Es gibt gute Gründe, die gegen die Vereinbarkeit dieser Vorschrift mit den Vorgaben der DSGVO zur Zusammenarbeit und Kohärenz sprechen. In jedem Falle aber besteht hier Klarstellungs- und Veränderungsbedarf (s. dazu bereits TB 2019 Rn. 21 f. und Rn. 136 ff.). Die unterbliebene Anhörung der RDSK-Mitglieder im Rahmen der Evaluation ist symptomatisch für das mangelnde Problembewusstsein des Bundes in Bezug auf die geforderte rechtliche Gleichordnung aller Aufsichtsbehörden nach Art. 51 DSGVO. Erwartungsgemäß äußert sich der im Oktober 2021 veröffentlichte Evaluationsbericht des BMI[44] dazu nicht.

65 Konkrete Konsequenzen hatte der Evaluationsbericht allerdings ohnehin nicht – wenig verwunderlich angesichts des unmittelbar anschließenden Wechsels der Bundesregierung. Ein ähnliches Schicksal könnte aus dem gleichen Grund zumindest partiell die im Januar 2021 verabschiedete **Datenstrategie**[45] der (vormaligen) Bundesregierung erleiden. Ihr Schwerpunkt liegt in besseren Rahmenbedingungen für die Nutzung von Daten für Zwecke der Forschung und Wissenschaft, aber auch für die Wirtschaft. Als eines der Ziele nennt sie eine rechtssichere und kohärente Ausgestaltung des Datenschutzrechts in Deutschland sowie eine engere Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder und verweist insoweit auf die Evaluation des BDSG.

66 Im Rahmen einer konzertierten Aktion hatten seit August 2020 mehrere Landesdatenschutzbehörden den **Einsatz von Cookies und die Einbindung von Drittdiensten auf den Webseiten von Medienunternehmen**[46] untersucht. Schwerpunkt war dabei das Nutzertra-

44 Bundesministerium des Innern, für Bau und Heimat (2021). Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/79 und zur Umsetzung der Richtlinie (EU) 2016/680 [Bericht], Oktober 2021, https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/downloads/berichte/evaluierung-bdsg.pdf [Stand: 25.02.2022].

45 Datenstrategie der Bundesregierung, Kabinettfassung vom 27. Januar 2021.

46 Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (2021, 30. Juni). Länderübergreifende Prüfung: Einwilligungen auf Webseiten von Medienunternehmen sind meist unwirksam – Nachbesserungen sind erforderlich [Pressemitteilung].

cking der Presseverlage zu Werbezwecken. Ende Juni 2021 informierten die beteiligten Landesdatenschutzbehörden über die wesentlichen Ergebnisse. Danach waren die meisten der geprüften Webseiten nicht DSGVO-konform. Die von den Webseiten abgefragte Einwilligung der Nutzer für die Verarbeitung ihrer personenbezogenen Daten sei in der Mehrheit der Fälle nicht wirksam, weil sie die Anforderungen des Art. 7 DSGVO bzw. der Rechtsprechung des EuGH nicht erfülle. Die im Rahmen des Nutzertrackings erhobenen personenbezogenen Daten würden insbesondere genutzt, um umfassende und seitenübergreifende Persönlichkeitsprofile zu generieren und anzureichern. Diese würden für das Onlinemarketing, insbesondere im Verfahren einer Echtzeitauktion von Werbeplätzen eingesetzt. Unter anderem hierin liegt ein entscheidender Unterschied zur Datenverarbeitung der Rundfunkanstalten bei der Nutzungsmessung ihrer Onlineangebote, die sie ausschließlich in anonymisierter Form und nur zu eigenen publizistischen Zwecken durchführen (s. dazu bereits TB 2020 Rn. 106).

67 Den seit 2017 verliehenen und mit 3.000 Euro dotierten **Datenschutz Medienpreis (DAME)**[47] erhielt für das Jahr 2020 ein Beitrag von Svea Eckert und Henning Wirtz für das „Funk"-Reportage-Format „STRG_F". Sie dokumentierten anschaulich die teils versteckte und nicht immer kontrollierbare Datenverarbeitung durch sogenannte Smartspeaker[48]. Und ein von einem Team des Bayerischen Rundfunks produzierter mehrteiliger Instagram-Beitrag gewann den mit 1.500 Euro dotierten Preis in der Kategorie „Social Media". Die Beteiligten deckten in einem Selbstversuch Schwachstellen in der bei Jugendlichen beliebten Dating App „Lovoo" auf. Wie im Vorjahr kamen damit zwei der drei ausgezeichneten Medienproduktionen mit Datenschutzthemen aus dem öffentlich-rechtlichen Rundfunk.

68 Verliehen wird der Datenschutz Medienpreis von einer Gemeinschaft mehrerer Organisationen, darunter die Datev Stiftung Zukunft, der Berufsverband der Datenschutzbeauftragten und die von den der Landesmedienanstalten aus Rheinland-Pfalz und Nordrhein-Westfalen getragene EU-Initiative Klicksafe. Prämiert werden sollen Beiträge, die Datenschutz anschaulich und verständlich erklären und dabei zugleich die Themen und Sprache ihrer Zielgruppe treffen. Für interessierte Medienschaffende bzw. Redaktionen kann die Aussicht auf einen solchen Preis eine zusätzliche Motivation dafür sein, sich des nur vordergründig sperrigen Themas Datenschutz anzunehmen und es zielgruppengerecht aufzubereiten. Im Idealfall wecken oder steigern sowohl die dabei entstehenden Beiträge als auch die Berichterstattung über die Preisverleihung die Sensibilität und Aufmerksamkeit für Fragen des Datenschutzes.

69 Mit Blick auf seine massiv zunehmende Bedeutung für jeden Einzelnen wie auch die Gesellschaft insgesamt gehört das Thema Datenschutz nach meinem Verständnis zum Kanon der Kernthemen, denen der öffentlich-rechtliche Rundfunk in seiner Berichterstattung besonderes Augenmerk widmen sollte. Zwar finden einschlägige Aspekte, wie die beiden

---

https://www.datenschutz.de/laenderuebergreifende-pruefung-einwilligungen-auf-webseiten-von-medienunternehmen-sind-meist-unwirksam-nachbesserungen-sind-erforderlich [Stand: 25.02.2022]

47 BvD e.V. (2021). Rückblick DAME 2020: And the winner is...Svea Eckert & Henning Wirtz. https://www.bvdnet.de/rueckblick-datenschutz-medienpreis-2020 [Stand: 25.02.2022]

48 Eckert, Svea; Wirtz, Henning (2020, 30. Juni). Smart Speaker Wobei Alexa, Siri & Co heimlich mithören [Video], https://www.youtube-nocookie.com/embed/BBkXKPfvyBI.

prämiierten Beiträge zeigen, durchaus immer wieder und in unterschiedlichsten Sendungen und Formaten Platz. Wünschenswert wäre aber – nicht anders als etwa beim Thema Klimaschutz oder Artensterben – eine Berichterstattung, die ebenso nachhaltig angelegt ist und wirkt wie die Entwicklung, um die es dabei geht.

70 Darüber hinaus sind die einschlägigen Beiträge in den jeweiligen Programmen oder auch Online bisher weder inhaltlich-strukturell noch gar senderübergreifend erschlossen und daher allenfalls über die Suchfunktion als „Einzelprodukt" auffindbar (dazu schon TB 2020 Rn. 49 sowie TB 2019 Rn. 174; siehe auch den Hinweis auf die Mediatheken auf meiner Website). Das wiederum funktioniert freilich nur, wenn der Titel des Beitrags überhaupt einen Bezug zum Datenschutz erkennen lässt. Für das an diesem Thema interessierte Publikum, aber auch für Bildungs- und Verbraucherschutzeinrichtungen wäre es deshalb ein erheblicher Mehrwert, wenn die Rundfunkanstalten in ihren Onlineangeboten bzw. Mediatheken die Auffindbarkeit von Inhalten mit Bezug zum Datenschutz erleichtern. Dazu könnten sie beispielsweise eine eigene Rubrik zu Datenschutzthemen einrichten, unter denen dann alle inhaltlich passenden Beiträge aus Hörfunk, Fernsehen und Online auffindbar und (je nach rundfunk- und urheberrechtlicher Verfügbarkeit) abrufbar wären, oder das entsprechende Angebot anderweitig – etwa durch eine deutlich differenziertere Suchfunktion als bisher - leichter erschließbar machen.

71 Solche Überlegungen liegen auch deshalb nahe, weil der öffentlich-rechtliche Rundfunk selbst infolge der diversifizierten Ausspiel- und Kommunikationswege zunehmend in datenschutzrechtlich besonders sensiblen Umgebungen bzw. auf problematischen Plattformen präsent ist und sie dadurch nicht zuletzt nolens volens auch aufwertet. Zudem manifestiert sich seine Orientierungsfunktion sowie sein Bildungsauftrag gerade in einer Berichterstattung, die über die anlass- und einzelfallbezogene Darstellung oder gar ein bloßes „Clickbaiting" hinausgeht und es ermöglicht, größere Zusammenhänge zu erkennen und gesellschaftliche Entwicklungen zu reflektieren. Dazu kann auch eine themenbezogene Bündelung und Aufbereitung unterschiedlichster Angebote zum Datenschutz in **multimedialen Dossiers oder Rubriken** beitragen. Ich würde es daher sehr begrüßen, wenn die Rundfunkanstalten mit Unterstützung der Gremien, die für die grundsätzlichen Fragen zur Programmgestaltung zuständig sind, ihre Angebots- bzw. Mediatheken-Strategie in diesem Sinne weiterentwickeln.

2 Der Gemeinsame Rundfunkdatenschutzbeauftragte

72 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 des öffentlich-rechtlichen Rundfunks insoweit der Rolle der Landtage im staatlichen Bereich. Sie soll verhindern, dass – anders als vor Inkrafttreten der DSGVO - der datenschutzrechtlich Verantwortliche (Intendant) bei der Besetzung der Aufsichtsposition formell mitwirkt.

73 Für den Bayerischen Rundfunk hat mich der Rundfunkrat mit Zustimmung des Verwaltungsrats (Art. 21 BR-Gesetz), für den Saarländischen Rundfunk (§ 42b SMG) und den Westdeut-

schen 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. Die vier- bzw. sechsjährige Amtszeit ergibt sich aus dem jeweiligen Landesrundfunk- oder Landesmediengesetz bzw. dem Deutschlandradio- und dem ZDF-Staatsvertrag.

74 Zu den Spezifika der Konstruktion der gemeinsamen Datenschutzaufsicht für fünf Rundfunkanstalten habe ich mich bereits früher (TB 2019 Rn. 106 ff.) ausführlich geäußert. Nahezu vier Jahre, nachdem die DSGVO wirksam geworden ist, und drei Jahre nach Übernahme dieser Funktion liegen ausreichende Erfahrungen für ein erstes Resümee vor (dazu unten Rn. 88 ff.). Zunächst aber ein Blick auf die Entwicklung im Berichtsjahr:

a Allgemeine Entwicklung

75 Erneut hat sich die Coronapandemie auf meine Aufsichtstätigkeit, abgesehen von den – wie überall – veränderten Arbeitsbedingungen kaum ausgewirkt. Von Erkrankungen waren wir nicht betroffen, ein neuerlicher Personalwechsel auf der Referentenposition hatte andere Gründe, und die früher üblichen Präsenztermine und -sitzungen fanden weit überwiegend virtuell statt. Unvermeidlich und nachteilig ist allerdings, dass Anzahl und Qualität der beruflichen Kontakte dadurch spürbar nachgelassen haben. Ähnlich wie noch so viele „Freundschaften", „Likes" und Chats in den sogenannten Sozialen Netzwerken die „analogen" Pendants nicht annähernd ersetzen können, gilt dies selbstverständlich auch im beruflichen Umfeld.

76 Auch im zweiten Pandemiejahr ist die Zahl der konkreten Beschwerden bemerkenswerterweise weiter zurückgegangen (s. zur Statistik auch unten Rn. 163 ff.); dafür waren etliche Petenten umso hartnäckiger. Und auch 2021 erreichten mich vergleichsweise wenige Corona-bedingte Anliegen. Das ist, wie ich hoffe, vor allem darauf zurückzuführen, dass die Verantwortlichen in meinem Zuständigkeitsbereich von ihren internen Datenschutzbeauftragten ausreichend und qualifiziert beraten wurden, sodass das Gros der entsprechenden Fragen ohne Rückversicherung bei der Aufsicht geklärt werden konnte. Es mag allerdings auch sein, dass die Existenz einer von den internen Datenschutzbeauftragten zu unterscheidenden eigenständigen Rundfunkdatenschutzaufsicht sich in den Rundfunkanstalten und Beteiligungsgesellschaften in den vergangenen drei Jahren noch nicht hinreichend herumgesprochen hat. Dazu kann auch die reduzierte Präsenz vor Ort beigetragen haben.

77 Die Tätigkeitsschwerpunkte haben sich im übrigen im Berichtsjahr nicht verändert. Meine Ressourcen liegen am unteren Ende des gerade noch Vertretbaren (s. TB 2019, Rn. 115 f.). Schon deshalb habe ich mich weiterhin auf die folgenden Aufgaben aus dem umfangreichen Katalog des Art. 57 Abs. 1 DSGVO konzentriert, von denen ich mich wiederum nur einigen vertieft widmen konnte:

- Anwendung der 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 mit anderen Aufsichtsbehörden (lit. g)
- Untersuchungen über Anwendung der DSGVO durchführen (lit. h)
- Maßgebliche Entwicklungen verfolgen (lit. i)
- Liste der Anwendungen anlegen, die eine Datenschutz-Folgenabschätzung erfordern (lit. k).

78 Den Kern der Aufsichtsfunktion sehe ich dadurch aber gewahrt, und erfreulicherweise gab es auch im Berichtsjahr keine kapazitätsbedingte Notsituation. Allerdings liegt das durchaus auch an einigen strukturell und individuell begründeten besonders günstigen Rahmenbedingungen, die nicht ohne weiteres fortschreibbar bzw. als dauerhaft selbstverständlich zu unterstellen sind.

b Zusammenarbeit in der RDSK

79 In der Rundfunkdatenschutzkonferenz (RDSK) tauschen sich seit 2019 die Datenschutzstellen mit Aufsichtsfunktion im öffentlich-rechtlichen Rundfunk aus. Mitglieder sind also formell insgesamt 12 Aufsichtsstellen, gleich, ob sie – wie in acht Fällen der jeweilige Rundfunkdatenschutzbeauftragte – für die gesamte Datenverarbeitung der Rundfunkanstalten und ihrer Beteiligungsunternehmen zuständig sind oder – wie in vier Fällen - nur für deren journalistische Datenverarbeitung. Inzwischen hat die RDSK nicht nur ein Logo, sondern auch eine eigene Homepage, über die zusätzlich zu den bestehenden Möglichkeiten (wie etwa über meine Infothek) unter anderem die Regularien, Beschlüsse und Positionspapiere abrufbar sind.

80 Im Berichtsjahr hat die RDSK unter meinem Vorsitz unter anderem Positionspapiere mit datenschutzrechtlichen Eckpunkten zum Einsatz sogenannter Kollaborationssysteme sowie zum Verständnis von § 18 BDSG und zur Zusammenarbeit mit der DSK verabschiedet. Ferner hatte der Bundesdatenschutzbeauftragte mir und Vertretern anderer „spezifischer Aufsichtsbehörden“ einen Fragebogen der EU-Kommission zur Evaluation der DSGVO übermittelt und Gelegenheit zur Stellungnahme im Rahmen des Verfahrens zur Abstimmung einer Antwort der nationalen Aufsichtsbehörden gegeben. Meine für die RDSK abgegebenen Anmerkungen haben weitestgehend Eingang in die vom Bundesdatenschutzbeauftragten versandte Antwort auf den Fragebogen gefunden.

81 Im übrigen habe ich die Verantwortlichen meines Zuständigkeitsbereichs im Januar förmlich darüber informiert, dass ich federführend die Datenschutzaufsicht über die von ihnen organisatorisch betreuten Gemeinschaftseinrichtungen ausübe. Grundlage dafür ist eine auf meine Veranlassung hin im Vorjahr geschlossene entsprechende Verwaltungsvereinbarung der RDSK-Mitglieder (TB 2020 Rn. 60).

c Zusammenarbeit mit sonstigen Aufsichtsbehörden

82 Seit 2019 findet regelmäßig zweimal jährlich ein Austausch der in der DSK zusammengeschlossenen staatlichen mit den (in § 18 Abs. 1 S. 4 BDSG) sogenannten „spezifischen“ Auf-

sichtsbehörden statt (ausführlich dazu TB 2019 Rn. 135 ff.). Diese Praxis wurde unter Federführung der aktuellen DSK-Vorsitzenden aus dem Saarland im Berichtsjahr in Gestalt zweier Videokonferenzen unverändert fortgesetzt. Inzwischen hat sich bei allen Beteiligten allerdings der Eindruck verfestigt, dass diese bislang eher informatorisch und retrospektiv angelegte Form des Austauschs wenig ertragreich ist. Auf meinen Vorschlag hin hat die RDSK ein Positionspapier zu diesem Thema verabschiedet, das ich der DSK-Vorsitzenden mit dem Ziel einer Verständigung über die künftige Ausgestaltung der Zusammenarbeit übersandt habe. Die DSK hat zugesagt, das Thema im Jahr 2022 – dann unter dem Vorsitz des Bundesdatenschutzbeauftragten – mit der RDSK und den anderen „spezifischen Aufsichtsbehörden" konstruktiv zu erörtern.

83 Zu den vertrauensbildenden Verabredungen gehört die Bereitschaft der DSK, bei Interesse eine Vertretung der RDSK in einem ihrer Arbeitskreise zu ermöglichen (TB 2019, Rn. 139 ff.). Auf dieser Grundlage habe ich im Berichtsjahr wieder an zwei – leider erneut nur virtuellen - Zusammenkünften des **AK Grundsatzfragen der DSK** teilgenommen. Dank der mir vorab zur Verfügung gestellten Beratungsunterlagen konnte ich mir einen Eindruck vom Diskussionsstand zu zahlreichen grundsätzlich bedeutsamen Themen verschaffen, die dieser Arbeitskreis für die abschließende Meinungsbildung in der DSK vor- und aufbereitet und die auch in meiner Aufsichtspraxis eine Rolle spielen. Zwar sieht der Gaststatus eine förmliche Beteiligung an der Meinungsbildung im Arbeitskreis naturgemäß nicht vor. Gleichwohl nutze ich bei entsprechendem Anlass die Gelegenheit für den einen oder anderen Hinweis oder Anmerkungen aus der Perspektive der Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk. Etliche der im AK Grundsatz für die DSK aufbereiteten Themen sind hingegen für die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk nicht oder nur von geringerem Interesse. Einige wenige interne Themen schließlich erörterten die Mitglieder des AK Grundsatz ohne mich und die weiteren Gäste.

84 Außerdem war die RDSK (durch den Kollegen des NDR) auch bei zwei Sitzungen des AK Medien der DSK sowie durch meine Referentin bei einer Sitzung des AK Technik vertreten. Für sinnvoll hielte ich außerdem eine Beteiligung am AK Datenschutz- und Medienkompetenz. Dieser ist allerdings leider seit mehreren Jahren nicht mehr aktiv.

85 Weiterhin nicht abschließend beantwortet ist die Frage, ob und wie die DSK die Rundfunkdatenschutzbeauftragten in die Agenda des **Europäischen Datenschutzausschusses** (EDSA)[49] einbezieht (s. TB 2019, Rn. 142). Immerhin hat die DSK frühzeitig die RDSK im Verfahren zur Abstimmung einer Antwort auf den Fragebogen der EU-Kommission zur Evaluation der DSGVO kontaktiert (oben Rn. 80). Dies ersetzt allerdings natürlich nicht eine strukturierte, verlässliche Beteiligung an Vorgängen, die im EDSA erörtert werden.

d Zusammenarbeit mit den internen Datenschutzbeauftragten

86 Meine mit Amtsantritt begonnene Praxis, mich wenigstens zweimal jährlich mit den Datenschutzbeauftragten der Rundfunkanstalten meines Zuständigkeitsbereichs sowie des Beitragsservice in einer sogenannten **5+1-Runde** auszutauschen, konnte ich umständehalber

[49] https://edpb.europa.eu/about-edpb/about-edpb_de

leider erneut nur mittels zweier Videoschaltkonferenzen fortführen. Wichtig ist mir aber, den Kolleginnen und Kollegen überhaupt die Möglichkeit zu geben, die für diesen Kreis insgesamt relevanten Vorgänge, mit denen sie jeweils befasst sind, in einer solchen überschaubaren Runde zur Diskussion zu stellen und gegebenenfalls eine Positionierung bzw. Klärung durch mich herbeizuführen. Umgekehrt erhalte ich selbst Hinweise auf aufsichtsrelevante Themen aus der betrieblichen Perspektive und informiere die Runde über Erfahrungen und Vorhaben aus meiner Aufsichtspraxis.

87 In unterschiedlicher Ausprägung beschäftigt alle Mitglieder dieser Runde nach wie vor die Konkretisierung ihrer Rechte und Pflichten im Verhältnis zum jeweils Verantwortlichen bzw. den mit datenschutzrelevanten Aufgaben befassten Fachbereichen. Dass die DSGVO insoweit im Vergleich zur früheren Rechtslage einige substanzielle Veränderungen bewirkt hat, muss sich noch im Bewusstsein – und den Regularien – einiger Verantwortlicher niederschlagen (s. dazu bereits TB 2019, Rn. 204 ff., 211 ff.). Hier hat mein Audit zum Verzeichnis der Verarbeitungstätigkeiten im Jahr 2020 (TB 2020 Rn. 136 ff.) einiges in Bewegung gebracht. Klärungsbedarf zeigte sich insoweit nicht nur in Bezug auf die Zuständigkeit für rechtlich unselbstständige Organisationseinheiten mehrerer gemeinsam Verantwortlicher (Gemeinschaftseinrichtungen), die eine Rundfunkanstalt für diese Gemeinschaft organisatorisch-administrativ betreut. Auch funktional, etwa im Verhältnis zu den Organen und bestimmten sonstigen der Rundfunkanstalt zugehörigen oder angegliederten Organisationseinheiten beförderte der Austausch ein gemeinsames Verständnis. Konkrete Beschwerden bzw. Streitfälle dazu haben mich allerdings im Berichtszeitraum nicht erreicht.

e Zwischenbilanz

88 Die bisherigen Erfahrungen mit der ersten gemeinsamen Datenschutzaufsicht gemäß Art. 51 DSGVO im öffentlich-rechtlichen Rundfunk sprechen dafür, diese Einrichtung mindestens zu verstetigen. Besser noch wäre es, diese Aufsichtsfunktion auch strukturell an einer Stelle zusammenzuführen, also als eine einzige Behörde auszugestalten; dazu bedürfte es freilich einer staatsvertraglichen Grundlage bzw. Rahmenvorgabe (s. dazu schon TB 2019 Rn. 110). Hinsichtlich der bisherigen Konstruktion des gemeinsamen RDSB hat sich in mehreren Punkten Konkretisierungs- oder Veränderungsbedarf gezeigt. Einige wesentliche Aspekte zur weiteren Perspektive sind deshalb zu berücksichtigen[50]. Sie beziehen sich auf die rechtlichen Grundlagen der Konstruktion, die Verortung in der Struktur und in den Regularien der Rundfunkanstalten sowie die Aufsichtspraxis:

89 (1) Klarstellung der gesetzlichen Grundlagen
Die bestehenden gesetzlichen Grundlagen zur Zuständigkeit sowie den Aufgaben und Befugnissen des Rundfunkdatenschutzbeauftragten von BR, SR, WDR, DRadio und ZDF sollten in folgenden Punkten ergänzt bzw. präzisiert werden:

- Die §§ 12 und 23 Abs. 1 MStV verweisen in Bezug auf die Aufsichtszuständigkeit für die Beteiligungsunternehmen auf die Vorschriften zur Prüfungsbefugnis der Rechnungshöfe. Dies ist erkennbar eine bloße Verlegenheitslösung. Die Gründe, die für eine rundfunkspezifische staatsunabhängige Datenschutzaufsicht maßgeblich sind, sprechen

[50] Zur Ausgangslage siehe ausführlich TB 2019 Rn. 106 ff.

dafür, deren Zuständigkeit weiter als die der Rechnungshöfe zu fassen. Sachgerecht ist es, die Aufsichtszuständigkeit ohne eine solche Verweisung eigenständig zu regeln.

- Dem RDSB fehlen – wie den staatlichen Datenschutzbehörden – Möglichkeiten, aufsichtsrechtlich angeordnete Abhilfemaßnahmen nach Art. 58 Abs. 2 DSGVO nötigenfalls mit Zwangsmitteln durchzusetzen. Dies kann auch die förmliche Beanstandung nicht ersetzen.
- Es sollte auf Landesebene jeweils ausdrücklich klargestellt werden, dass für die Aufsicht über die Umsetzung der in der Praxis besonders bedeutsamen Vorschriften des § 25 TTDSG durch Rundfunkanstalten und deren Beteiligungsunternehmen der RDSB zuständig ist (s. dazu oben Rn. 21, 28).

90 (2) Organisatorische Verselbstständigung
Nach den seit Mai 2018 geltenden Vorgaben fungiert der RDSB im Gegensatz zur früheren Rechtslage nicht mehr als „interne Aufsicht" der Rundfunkanstalten. Zwar ist er Teil des staatsunabhängigen öffentlich-rechtlichen Rundfunks, aber als seinerseits unabhängige Instanz nicht Teil der Rundfunkanstalt selbst. Insbesondere ist er weder viertes Organ noch interne Abteilung der Rundfunkanstalt. Er kontrolliert den Datenschutz nicht in deren Auftrag (bzw. dem der Gremien), sondern qua Gesetz. Soweit nach Landesrecht seine Dienststelle bei der Geschäftsstelle der Gremien einzurichten ist, handelt es sich um eine rein formale Zuordnung. Sie trägt lediglich dem Umstand Rechnung, dass die Aufsichtsbehörde überhaupt im Organisationsgefüge einer Rundfunkanstalt verortet sein muss. Dies bedeutet nicht, dass der Behördensitz dem der Gremiengeschäftsstelle oder auch nur dem der Rundfunkanstalt entsprechen muss. Im Gegenteil: eine organisatorische und/oder räumliche Distanz unterstreicht die Unabhängigkeit im Außenverhältnis.

91 (3) Keine Gemeinschaftseinrichtung
Ihre völlige Unabhängigkeit unterscheidet die gemeinsame Datenschutzaufsicht signifikant von den sogenannten Gemeinschaftseinrichtungen (GSEA) der Rundfunkanstalten. Die auf solche GSEA zugeschnittenen Verwaltungsregelungen und Verfahrensabläufe sind mit der Unabhängigkeit der gemeinsamen Datenschutzaufsicht nicht vereinbar.

92 (4) Unabhängige Etat- und Personalverantwortung sowie Geschäftsführung
Die internen Regularien der Rundfunkanstalt(en) gelten für die Aufsichtsbehörde nicht per se. Grundsätzlich muss die landesrechtlich vorgesehene Satzung alle Fragen zur konkreten Gewährleistung ihrer Unabhängigkeit regeln; dies ist bislang nicht vollständig geschehen. In jedem Fall sind solche Regularien nur insoweit anwendbar, als sie die Unabhängigkeit nicht beeinträchtigen. Der RDSB muss in allen Angelegenheiten, die die Ausstattung und Ressourcen seiner Aufsichtsbehörde betreffen, Subjekt und darf nicht nur Objekt entsprechender interner Verfahren sein. Nur er, nicht die Rundfunkanstalt hat seinen Wirtschafts- und Stellenplan gegenüber den zuständigen Gremien zu vertreten. Fachbereiche der Rundfunkanstalt dürfen einschlägige Entscheidungen weder beeinflussen noch gar (für den RDSB) treffen. Die fachliche Arbeitgeberfunktion hat ausschließlich der RDSB, nur er darf daher beispielsweise das Arbeitszeugnis für die bei ihm Beschäftigten ausstellen, Urlaub oder Fortbildungen genehmigen etc. Interne Abstimmungs- oder Genehmigungsvorbehalte im Verhältnis zur internen Hierarchie der Rundfunkanstalt einschließlich deren Intendantin (etwa in Bezug auf Dienstreisen, Beschaffungen, Urlaub etc.) sind für die Aufsichtsbehörde unbeachtlich. Sie ist nicht Teil der internen Organisationsstruktur der Rundfunkanstalt,

deshalb haben deren Belegschafts- bzw. Interessenvertretungen in ihren Angelegenheiten weder Informations- noch Beteiligungsrechte.

93 (5) Planungssicherheit und Qualitätssicherung
Die gesetzlichen Anforderungen an eine Aufsichtsbehörde nach Art. 51 DSGVO sind nur mit qualifiziertem Personal einzulösen. Dies erfordert eine längerfristige Perspektive. Das in der Aufsichtsbehörde beschäftigte Personal muss daher grundsätzlich auch unbefristet angestellt werden können. Ohne eine langfristige Standortfestlegung ist dies nicht möglich. Auch die sonstigen Rahmenbedingungen müssen die realistische Aussicht eröffnen, qualifiziertes Personal gewinnen und für längere Zeit binden zu können. Wenn die Beschäftigungsbedingungen für vergleichbare Tätigkeiten in der Rundfunkanstalt bzw. im unmittelbaren Umfeld günstiger sind, unterläuft dies die Aufsichtsfunktion.

94 (6) Keine Kontrollrechte der Rundfunkanstalt oder Dritter
Die Rundfunkanstalt hat keine Kontrollrechte gegenüber der Aufsichtsbehörde. Das Hausrecht über die von ihr genutzten Räume steht ausschließlich dem RDSB selbst zu. Interne Abteilungen der Rundfunkanstalt haben nur mit seiner Einwilligung Zugang zur Infrastruktur, zu Unterlagen und Daten der Aufsichtsbehörde. Anderes gilt allenfalls für Prüfungen, die der Verwaltungsrat (etwa durch die Interne Revision der Rundfunkanstalt) ausdrücklich beauftragt, soweit er dabei wiederum die gesetzlichen Grenzen seiner Kontrollbefugnisse wahrt. Die Satzung (oben 4) muss eine solche Möglichkeit vorsehen und das dabei anzuwendende Verfahren regeln.

95 (7) Präsenz und Tätigkeitsbericht
Die Datenschutzaufsicht muss ihre Öffentlichkeitsarbeit und Kommunikation vollständig eigenständig, unabhängig von der Rundfunkanstalt, gestalten können. Jede Maßnahme oder Aktivität, die im Außenverhältnis den Eindruck erweckt, die Datenschutzaufsichtsbehörde sei eine Untergliederung der Rundfunkanstalt oder vertrete diese in Datenschutzangelegenheiten, ist nach Art 52 DSGVO unzulässig. Der Tätigkeitsbericht des RDSB ist der einer von der Rundfunkanstalt vollständig unabhängigen Aufsichtsbehörde und daher nicht mit Berichten interner Stellen oder sonstiger Beauftragter bzw. Einrichtungen der Rundfunkanstalten vergleichbar. Insbesondere handelt es sich nicht um einen Bericht „der Rundfunkanstalt“. Deren Organe sind (neben der Öffentlichkeit sowie den Parlamenten und Regierungen der Bundesländer, s.o. Rn. 1 ff.) Adressaten, aber nicht Auftraggeber des Berichts.

3 Schwerpunktthemen der eigenen Praxis

96 Viele Vorgänge des Berichtsjahrs betrafen Fragen, die bereits Gegenstand früherer Verfahren waren, die ich daher schon geprüft und in einem meiner bisherigen Tätigkeitsberichte dargestellt habe. Im folgenden gehe ich deshalb nur auf jene ein, die zumindest auch neue Fragen grundsätzlicher Natur aufwarfen oder in denen über neue Entwicklungen zu berichten ist.

a Beauftragung Inkassounternehmen im Beitragseinzugsverfahren

97 Mehrfach beanstandeten Petenten, dass der Zentrale Beitragsservice (ZBS) ihre personenbezogenen Daten für den Einzug ausstehender Beitragszahlungen ohne ihre Kenntnis an Inkassounternehmen übermittelt habe. Die Prüfung der Grundlagen einer solchen Beauftragung sowie der dabei zu berücksichtigenden datenschutzrechtlichen Belange hat in keinem Fall Hinweise auf eine Datenschutzverletzung durch den Beitragsservice ergeben.

98 Der ZBS führt als gemeinsame Verwaltungseinrichtung im Auftrag der jeweils zuständigen Landesrundfunkanstalt das Verfahren zur Feststellung und Abwicklung der Beitragspflicht durch. Grundlage dafür sind die Vorschriften des Rundfunkbeitragsstaatsvertrags der Länder (RBStV) sowie der Satzung über das Verfahren zur Leistung der Rundfunkbeiträge (Beitragssatzung) der jeweils zuständigen Landesrundfunkanstalt. Diese ist gemäß § 10 Abs. 7 S. 2 RBStV ermächtigt, einzelne Tätigkeiten bei der Durchführung des Beitragseinzugs und bei der Ermittlung von Beitragsschuldnern auf Dritte zu übertragen und das Nähere durch eine Satzung zu regeln.

99 Gem. § 9 Abs. 2 RBStV in Verbindung mit § 16 der jeweiligen Beitragssatzung dürfen die Landesrundfunkanstalten Dritte beauftragen, unter anderem mit Inkassomaßnahmen ausstehende Rundfunkbeiträge einschließlich aller Nebenforderungen einzutreiben. In datenschutzrechtlicher Hinsicht wird ein solches Unternehmen dann auf der Grundlage eines Vertrages gemäß Art. 28 DSGVO als Auftragsverarbeiter der jeweiligen Landesrundfunkanstalt bzw. des für sie handelnden ZBS tätig, Art. 4 Nr. 8 DSGVO. Es ist damit nicht „Dritter“ im Sinne von Art. 4 Nr. 10 DSGVO, sondern handelt nach Maßgabe des Vertrags gemäß Art. 28 DSGVO wie der Verantwortliche (also die jeweilige Landesrundfunkanstalt bzw. der von ihr beauftragte Beitragsservice) selbst. Aus dem gleichen Grund findet zwischen dem ZBS und dem beauftragten Inkassounternehmen auch keine Datenverarbeitung (insbesondere Datenübermittlung) statt, die einer eigenen Rechtsgrundlage im Sinne von Art. 6 DSGVO, insbesondere einer Einwilligung der betroffenen Person bedürfte. Über die etwaige Datenweitergabe an einen Inkassodienstleister informiert der ZBS in seinen allgemeinen Datenschutzhinweisen. Damit sind grundsätzlich die sich aus Art. 13 bzw. 14 DSGVO ergebenden Anforderungen an eine hinreichende Information über die im Zuge des Beitragsverfahrens stattfindende Datenverarbeitung erfüllt.

100 Der vom ZBS beauftragte Auftragsverarbeiter unterliegt der Aufsicht der für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzaufsichtsbehörde, die bei entsprechenden konkreten Anhaltspunkten zu überprüfen hat, ob er die gebotenen technischen und organisatorischen Maßnahmen zum Schutz und zur Sicherheit der personenbezogenen Daten nicht oder nicht ausreichend ergriffen hat. Gleiches gilt für jeden sonstigen etwaigen Datenschutzverstoß im Zusammenhang mit dem Inkassoauftrag. Hingegen ist es keine datenschutzrechtliche Frage, ob der ZBS selbst oder das von ihm beauftragte Inkassounternehmen die aus den beitragsrechtlichen Vorgaben folgenden Voraussetzungen für einen solchen Inkassoauftrag erfüllt. Dies muss die betroffene Person nötigenfalls im Klageweg unmittelbar im Verhältnis zur jeweiligen Landesrundfunkanstalt bzw. dem in ihrem Auftrag handelnden ZBS klären.

b Berichtigung von „Altdaten“

101 In einem Beschwerdeverfahren hatte der Petent den ZBS mehrfach vergeblich aufgefordert, eine in seinem Beitragskonto gespeicherte fehlerhafte frühere Meldeadresse zu berichtigen. Der ZBS lehnte dies mit der Begründung ab, der betreffende Zeitraum liege weit in der Vergangenheit, und er speichere die Daten lediglich mit Rücksicht auf die gesetzlichen Aufbewahrungspflichten, nach deren Ablauf er sie ohnehin löschen werde. Eine etwaige Berichtigung habe keinerlei Auswirkungen mehr auf die Frage der Rechtmäßigkeit der damaligen Beitragsfestsetzung.

102 Gemäß Art. 16 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender personenbezogener Daten zu verlangen. Wenn dieser Anspruch darauf abzielt, einen vollständig datenschutzrechtskonformen Zustand zu ermöglichen, bezieht er sich abstrakt-generell auf alle objektiv unrichtigen Daten. Nach diesem Verständnis kommt es dann konsequenterweise weder auf die Relevanz oder den Umfang der Unrichtigkeit noch auf ein Berichtigungsinteresse an.

103 Wenn der Berichtigungsanspruch hingegen „nur“ eine zutreffende, faire und transparente Datenverarbeitung durchsetzen soll, ist entscheidend, ob der Verantwortliche die Daten noch für seine Verarbeitungstätigkeiten benötigt: Die Daten müssten gem. Art. 5 Abs. 1 lit. d) DSGVO im Hinblick auf die „Zwecke ihrer Verarbeitung“ unrichtig sein, und ihre weitere Verarbeitung müsste das Grundrecht der betroffenen Person auf Datenschutz tangieren.

104 Für dieses Verständnis spricht, dass Art. 5 Abs. 1 lit. d) DSGVO voraussetzt, dass der Verantwortliche überhaupt noch eine Verarbeitung beabsichtigt (die über die bloße Speicherung hinausgeht). Wenn dies – wie in dem Beschwerdefall - gar nicht mehr vorgesehen und zudem auch nicht mehr statthaft ist, fehlt jeder Bezug zu einer potentiellen Verarbeitung, die die rechtlichen Interessen des Betroffenen beeinträchtigen könnte. Ziel der datenschutzrechtlichen Vorschriften kann es schwerlich sein, einen vollständig objektiv zutreffenden Datenbestand zu garantieren, sondern „nur“, eine objektiv zutreffende Datenverarbeitung zu erwirken. Allerdings sind Anhaltspunkte für ein wie immer geartetes „Rechtsschutzbedürfnis“ des Betroffenen der DSGVO jedenfalls nicht ohne weiteres zu entnehmen. Verbindlich kann nur der EuGH die Reichweite des Berichtigungsanspruchs definieren.

105 Im betreffenden Beschwerdefall konnte ich die Streitfrage offenlassen. Denn der ZBS kündigte an, dass die Löschung des Beitragskontos ohnehin unmittelbar bevorstehe. Den Petenten habe ich über meine Bewertung der Rechtslage sowie die bevorstehende Löschung informiert und veranlasst, dass er anschließend eine Nachricht des ZBS über den Vollzug erhielt.

c Verhältnis beitrags- zu datenschutzrechtlichen Fragen

106 Immer wieder geht es in Beschwerdefällen gegenüber dem ZBS darum, beitragsrechtliche von datenschutzrechtlichen Fragen abzugrenzen; nur letztere darf die Datenschutzaufsichtsbehörde prüfen. Beispielhaft sei hier ein bezeichnender, wenngleich ungewöhnlicher

Fall genannt, in dem eine Person eine Mahnung wegen vermeintlicher Zahlungsrückstände über mehrere Jahre für ein Beitragskonto erhalten hatte, von dessen Existenz sie erst durch das Mahnschreiben erfuhr. Auf ihre Reklamation hin stornierte der ZBS rückwirkend das Beitragskonto und die Beitragsforderungen. Zugleich lehnte er einen Antrag auf Akteneinsicht zu dem betreffenden Beitragskonto ab. Mit ihrer Beschwerde nach Art. 77 DSGVO machte die Person eine fehlerhafte Verarbeitung der sie betreffenden personenbezogenen Daten und eine Verletzung der Transparenzverpflichtungen durch den ZBS geltend.

107 Bei der Prüfung stellte sich heraus, dass der ZBS im Rahmen einer Adressklärung die aktuellen Daten einer Person abgefragt hatte, die einen ähnlichen Vor-, aber denselben Nachnamen und dasselbe Geburtsdatum wie die betroffene Person hatte. Vom Einwohnermeldeamt erhielt der ZBS daraufhin allerdings fälschlicherweise die (nahezu identischen) Daten des Petenten. Dem ZBS fiel der unterschiedliche Vorname nicht auf und er ordnete den Datensatz versehentlich dem Beitragskonto der anderen Person zu, auf die sich die Adressanfrage bezogen hatte. Erst auf den Widerspruch des Petenten gegen die Zahlung der vermeintlich rückständigen Beitragsforderungen bemerkte der ZBS das Versehen und machte die auf dessen Namen lautende fehlerhafte Feststellung der Beitragspflicht durch die rückwirkende Abmeldung des dafür eingerichteten Beitragskontos wieder rückgängig.

108 Auslöser des Vorgangs war also, dass der ZBS die betroffene Person zu Unrecht für beitragspflichtig gehalten hatte. Das lag auch an einer eigenen fehlerhaften Datenverarbeitung. Diese war allerdings nur die Folge eines beitragsrechtlich veranlassten Vorgehens, das der Klärung eines (vermeintlichen) Beitragssachverhalts diente. Im Vordergrund stand also die Frage, ob der ZBS die einschlägigen Vorschriften des RBStV sowie der Beitragssatzung ordnungsgemäß angewandt hatte. Dies hätte die betroffene Person nötigenfalls im Wege des Widerspruchs gegen einen gegen sie ergangenen Festsetzungsbescheid bzw. durch eine entsprechende Klage feststellen lassen können.

109 Demgegenüber sind die datenschutzrechtlichen Aspekte dieser fehlerhaften Datenverarbeitung nachrangig und können nicht kumulativ oder alternativ Gegenstand eines aufsichtsbehördlichen Verfahrens sein. Anderenfalls wäre in letzter Konsequenz nahezu jeder fehlerhafte Verwaltungsbescheid gegen eine natürliche Person auf einen Datenschutzverstoß zurückzuführen. Die Datenschutzaufsicht hat aber nicht das gesamte Verwaltungshandeln bzw. die Rechtmäßigkeit der damit verbundenen Datenverarbeitung zu überprüfen, sondern lediglich, ob die Verwaltung – hier: der ZBS – die spezifischen Vorgaben der DSGVO zur Ordnungsgemäßheit ihrer Datenverarbeitung sowie die sich aus den Artt. 12 ff. DSGVO ergebenden Betroffenenrechte wahrt. Zu diesen gehört wiederum kein Anspruch auf Akteneinsicht, wie ihn die betroffene Person hier erhoben hatte, sondern nur das Auskunftsrecht nach Art. 15 DSGVO bzw. § 11 Abs. 8 RBStV. Ein von mir zu sanktionierender eigenständiger Datenschutzverstoß lag hier mithin nicht vor. Der betroffenen Person genügte aber meine ausführliche Erläuterung der Sach- und Rechtslage.

d Arbeitnehmerüberlassung und Gemeinsame Verantwortung

110 Um das Verhältnis zwischen Datenschutzrecht und sachverhaltsspezifischen Vorschriften geht es auch bei der Frage, ob im Falle einer Arbeitnehmerüberlassung Ver- und Entleiher für die mit der Abwicklung des Vertrages verbundene Verarbeitung des Leiharbeitnehmers gemeinsam verantwortlich sind. In diesem Fall müssten sie neben dem Überlassungsvertrag auch einen solchen nach Art. 26 DSGVO schließen. Dies sehe ich jedoch grundsätzlich als nicht erforderlich an. Der Regelfall ist dadurch gekennzeichnet, dass die einzige Verbindung zwischen dem Ver- und dem Entleiher die Überlassung von Personal ist, das für den jeweils festgelegten Zeitraum in den Betrieb des Entleihers eingegliedert ist und seine Arbeit allein nach den Weisungen des Entleihers in dessen Interesse ausführt. Notwendiger Inhalt eines Arbeitnehmerüberlassungsvertrags ist die Verpflichtung des Verleihers gegenüber dem Entleiher, diesem zur Förderung von dessen Betriebszwecken Arbeitnehmer zur Verfügung zu stellen. Die Vertragspflicht des Verleihers gegenüber dem Entleiher endet, wenn er den Arbeitnehmer ausgewählt und ihn dem Entleiher zur Verfügung gestellt hat.

111 Dabei unterfällt nicht jeder in diesem Sinne drittbezogene Arbeitseinsatz dem Arbeitnehmerüberlassungsgesetz. Arbeitnehmerüberlassung ist vielmehr durch eine spezifische Ausgestaltung der Vertragsbeziehungen zwischen Verleiher und Entleiher einerseits (dem Arbeitnehmerüberlassungsvertrag) und zwischen Verleiher und Arbeitnehmer andererseits (dem Leiharbeitsvertrag) sowie durch das Fehlen einer arbeitsvertraglichen Beziehung zwischen Arbeitnehmer und Entleiher gekennzeichnet. In dieser Konstellation verfolgt jeder der beteiligten Verantwortlichen eigene Interessen und verarbeitet die in diesem Zusammenhang anfallenden personenbezogenen Daten daher auch ausschließlich zu jeweils eigenen Zwecken. Bedingung für eine gemeinsame Verantwortlichkeit im Sinne des Art. 26 DSGVO ist jedoch, dass die Vertragspartner Zwecke und Mittel der Datenverarbeitung gemeinsam festlegen. Allein die „Durchführung der Arbeitnehmerüberlassung“ sehe ich nicht als hinreichenden übergeordneten „gemeinsamen Zweck“ an, da damit im Grunde auch jedes sonstige Vertragsverhältnis, das mit der Verarbeitung personenbezogener Daten verbunden ist, unter Art. 26 DSGVO zu subsumieren wäre.

112 Allerdings kann es durchaus bestimmte Konstellationen geben, in denen auch eine Arbeitnehmerüberlassung den Abschluss eines Vertrags nach Art. 26 DSGVO erfordert. Dies dürfte in erster Linie dort in Frage kommen, wo Ver- und Entleiher über das Verleihgeschäft hinaus gemeinsame (wirtschaftliche oder sonstige) Interessen verfolgen, die sich auch auf die Datenverarbeitung auswirken. Insbesondere etwa dort, wo die Arbeitnehmerüberlassung zwischen den beteiligten Verantwortlichen unter dem Dach eines Konzerns stattfindet, und hier vor allem sicherlich in solchen Fällen, in denen eine dafür eingerichtete zentrale Stelle die Personaldaten der im Konzern Beschäftigten verarbeitet. Eine solche Konstellation wäre unter Umständen im Verbund der in der ARD zusammengeschlossenen Rundfunkanstalten und ansonsten im Bereich der Beteiligungsunternehmen vorstellbar, soweit diese in einer Holdingstruktur organisiert sind.

e Nutzung „Sozialer Medien“

113 Dass die Rundfunkanstalten im Bestreben, die Bevölkerung, insbesondere jüngere Zielgruppen, auch über die sogenannten „Social Media“-Kanäle zu erreichen, die damit verbundenen datenschutzrechtlichen Aspekte nicht vernachlässigen dürfen, habe ich bereits ausführlich dargelegt (TB 2020 Rn. 95 ff.). Zahlreiche Anfragen oder Beschwerden legen Zeugnis davon ab, dass dieses Thema dauerhaft viele Nutzer der Onlineangebote des öffentlich-rechtlichen Rundfunks beschäftigt.

114 Nach meiner Auffassung sind die Rundfunkanstalten gehalten, sorgfältig zu begründen und die Nutzer darüber zu informieren, warum sie sich zur Erfüllung ihres Programmauftrags veranlasst sehen, die jeweiligen Plattformen zu nutzen und dort ihre Inhalte zu verbreiten. Sie müssen darlegen, auf welche Rechtsgrundlage sie sich insoweit stützen und warum ihre Belange die der betroffenen Personen überwiegen. Auf beiden Seiten sind dabei rechtliche Interessen zu berücksichtigen, die durch die Europäische Grundrechtecharta (GRCh), die DSGVO und das GG geschützt sind. Zudem haben die Rundfunkanstalten auf den Abschluss einer Vereinbarung mit dem – in aller Regel in den USA oder einem anderen Drittstaat ansässigen - Plattformanbieter hinzuwirken, die den Anforderungen von Art. 26 DSGVO genügt und die in den Drittstaat übermittelten personenbezogenen Daten in vergleichbarer Weise wie die DSGVO schützt. Ihre entsprechenden Aktivitäten müssen sie dokumentieren und ihre Nutzer über alle relevanten Umstände der durch sie veranlassten Datenverarbeitung informieren.

115 Die diesem Verständnis zugrunde liegenden Überlegungen habe ich in einem Positionspapier mit Empfehlungen zur Nutzung von Facebook-Fanpages durch die Rundfunkanstalten zusammengefasst, das auch in der Infothek meiner Website zum Abruf zur Verfügung steht. Es bewegt sich auf der Linie, die sich auch der aktuellen Rechtsprechung zur gemeinsamen Verantwortung zwischen Fanpage-Betreiber und Facebook – zuletzt dem Urteil des OVG Schleswig-Holstein vom 25.11.2021 (dazu oben Rn. 47) – entnehmen lässt. Im Vergleich zu dem dort entschiedenen Sachverhalt haben sich die Anforderungen an ein datenschutzkonformes Handeln der für die Datenverarbeitung durch „Soziale Medien“ Mitverantwortlichen allerdings insoweit noch verschärft, als die damit unvermeidlich verbundene Datenübermittlung in Drittstaaten, insbesondere die USA, nicht mehr pauschal durch den Hinweis auf das „Privacy Shield“-Abkommen „freigezeichnet“ werden kann.

116 Der Vollständigkeit halber sei noch erwähnt, dass die RDSK im Februar 2021 auch eine Entschließung zur AudioApp „Clubhouse“ verabschiedet hat. Das Interesse an und die Nachfrage nach dieser App erwies sich, ebenso wie ihre publizistische Relevanz, allerdings rasch als sehr kurzlebiges Phänomen, sodass eine intensivere Befassung mit ihr entbehrlich war. Der Tenor des RDSK-Papiers beschränkt sich denn auch auf die Vorgabe, die Installation der App auf allen dienstlich zur Verfügung gestellten Geräten, mindestens aber deren Zugriff auf das dienstliche Kontaktverzeichnis wirksam zu unterbinden. Gleiches muss im übrigen für jede App gelten, die – wie etwa WhatsApp, Instagram oder TikTok - darauf angelegt ist, auf die im jeweiligen Gerät gespeicherten Kontaktdaten zuzugreifen.

f Verarbeitung von Nutzungsdaten

117 Ein weiteres anhaltendes Dauerthema in meiner Aufsichtspraxis ist der Einsatz von Cookies für die Nutzungsmessung der Rundfunkanstalten (s. zuletzt TB 2020 Rn, 104 ff.). Das Inkrafttreten des TTDSG am 1. Dezember 2021 (oben Rn. 18 ff.) hat zwar die Rechtslage insoweit verändert und einen neuen Schub an Anfragen und Beschwerden ausgelöst. Die bisherige Praxis der Rundfunkanstalten bleibt jedoch weiterhin zulässig:

118 Nach der neuen Vorschrift des § 25 Abs. 1 S. 1 TTDSG ist „die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, … nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat." Das bedeutet: Cookies darf ein Onlineanbieter auf einem mobilen oder stationären Gerät grundsätzlich nur ablegen, wenn dessen Nutzer sich damit ausdrücklich einverstanden erklärt hat. Die Vorschrift transformiert, anders als der nun ersetzte § 15 TMG, nahezu wortidentisch Art. 5 Abs. 3 ePrivacy-Richtlinie in deutsches Recht. Sie dient dem Schutz der Privatsphäre und geht deshalb den Regelungen des Art. 6 DSGVO vor, die den Einsatz von Cookies auch auf der Basis einer der dort genannten gesetzlichen Grundlagen ermöglichen würden (s. bereits oben Rn. 19).

119 Insbesondere greift die Vorschrift also zunächst einmal unabhängig davon ein, dass die Rundfunkanstalten für ihre Nutzungsmessung nur vollständig anonymisierte Datenbestände auswerten. Denn auf einen Personenbezug der durch das jeweilige Cookie veranlassten Datenverarbeitung kommt es, anders als nach Art. 6 DSGVO, gerade nicht an. Und auch dass diese Datenverarbeitung journalistischen Zwecken dient, ist unerheblich. Denn das sogenannte „Medienprivileg" ist zumindest bislang seinerseits nur in Bezug auf das Recht auf Datenschutz ausgestaltet und rechtfertigt keine Freistellung von den Vorschriften zum Schutz der Privatsphäre.

120 Die Einwilligung ist gem. § 25 Abs. 2 TTDSG nur in zwei sehr eng begrenzten Ausnahmefällen entbehrlich. Insbesondere kommt das in Betracht, wenn der Einsatz der Cookies „unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann."

121 Insoweit ist zum einen zu berücksichtigen, dass Rezeption und Wirkung von Medienangeboten generell zu einem wesentlichen Teil davon abhängen, wie sie gestaltet sind und wann sie in welcher Form erscheinen. Das BVerfG bezeichnet die Medien (Presse wie Rundfunk) als „Medium und Faktor" der öffentlichen Meinungsbildung und beschreibt damit die diesem Prozess immanente Wechselwirkung nicht nur im Verhältnis zwischen Medium und Rezipienten, sondern auch zwischen den Medien selbst. Unterschiedlichste Formen der Nutzungsmessung (wie etwa die halbjährliche Marktanalyse – MA – im linearen Hörfunk oder die tägliche GfK-Marktanteilsmessung im linearen Fernsehen) gehören daher seit jeher zu den Mitteln der Positionierung gegenüber den publizistischen Wettbewerbern. Die Bedeutung der Nutzungsmessung für den publizistischen Erfolg, also die Relevanz redaktioneller Angebote hat sich im Wettbewerb der redaktionellen Telemedien noch einmal deutlich erhöht: in der nahezu unüberschaubaren Umgebung des Internets sind Aspekte wie Wahrnehmbarkeit, Präsenz, Aktualität und Nutzerfreundlichkeit für den Erfolg eines

Angebots besonders bedeutsam. Diese wiederum hängen von unterschiedlichsten Faktoren der Konfiguration, Gestaltung, Platzierung und Formulierung der einzelnen Inhalte eines Gesamtangebots ab, die wiederum je für sich erfasst und ausgewertet werden müssen. Wenn die dafür erforderliche Datenverarbeitung stets von der Einwilligung des Nutzers abhängig wäre, wäre mit hoher Wahrscheinlichkeit eine gewissermaßen objektive, nämlich repräsentative und damit hinreichend aussagekräftige Nutzungsmessung nicht mehr möglich.

122 Zum anderen beteiligen sich die Rundfunkanstalten am publizistischen Wettbewerb der elektronischen Medien im Internet nicht aus wirtschaftlichen oder sonstigen privatnützigen Gründen, sondern weil sie ihren verfassungsrechtlich verankerten und im Medienstaatsvertrag konkretisierten Funktionsauftrag wahrnehmen. Ausschließlich diesem dient die zu Zwecken der Nutzungsmessung durchgeführte Datenverarbeitung. Sie führt weder zu wie auch immer gearteten personalisierbaren Nutzungsprofilen, noch verwerten die Rundfunkanstalten die Daten selbst kommerziell oder stellen sie gar Dritten für solche Zwecke zur Verfügung. Vielmehr ermöglicht die Datenverarbeitung eine ausschließlich im publizistischen Interesse stattfindende inhalte- bzw. angebotsbezogene statistische Auswertung der Gesamtnutzung des Telemedienangebots und darauf basierende, journalistischen Zielen dienende Maßnahmen.

123 Schließlich muss die Datenverarbeitung auch gerade dafür erforderlich sein, einen „vom Nutzer ausdrücklich gewünschten Telemediendienst“ zur Verfügung zu stellen. Dem Wortlaut nach bezieht sich die Erforderlichkeit also auf den individuellen Wunsch des Nutzers, dem der Telemedienanbieter nicht anders als mithilfe der konkret – hier: für die anonymisierte Nutzungsmessung - eingesetzten Verarbeitungsvorgänge Rechnung tragen kann. Allerdings wird man die Vorschrift nicht so verstehen können, dass der jeweilige Nutzer sich ausdrücklich positiv zur betreffenden Datenverarbeitung verhalten haben muss. Denn dies entspräche letztlich dem Einwilligungserfordernis, das § 25 Abs. 2 Nr. 2 TTDSG (bzw. Art. 5 Abs. 3 ePrivacy-Richtlinie) in diesem Ausnahmefall gerade ausschließen will. Vielmehr soll sich der Wunsch des Nutzers gleichsam objektiv auf das Telemedienangebot beziehen, das die Rundfunkanstalten mithilfe der Nutzungsmessung zur Verfügung stellen.

124 Insoweit fällt ins Gewicht, dass das öffentlich-rechtliche Onlineangebot aus dem Rundfunkbeitrag finanziert ist. Der einzelne Beitragszahler kann zwar nicht verlangen, dass dieses Angebot seine individuellen Interessen und Präferenzen vollständig berücksichtigt und bedient. Wohl aber kann er erwarten, dass der öffentlich-rechtliche Rundfunk mit den ihm zur Verfügung stehenden Beitragseinnahmen ein im publizistischen Wettbewerb bestmöglich konkurrenzfähiges Angebot zur Verfügung stellt. Dies bedingt die Möglichkeit der Rundfunkanstalten, alle Erkenntnismöglichkeiten zur Wirkung, Reichweite und Akzeptanz ihrer Inhalte auszuschöpfen und das Angebot im publizistischen Wettbewerb stetig weiterzuentwickeln. Zu diesen Erkenntnismöglichkeiten gehört es auch, dass die Rundfunkanstalten auf einer aggregierten und damit gleichsam objektivierten Ebene die individuelle Interessenlage aller Nutzer erfassen. Insofern ist die zu Zwecken der Nutzungsmessung durchgeführte Datenverarbeitung mithin für den öffentlich-rechtlichen Rundfunk unbedingt erforderlich, um einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung zu stellen.

125 In diesem Sinne habe ich die seit Inkrafttreten des TTDSG wieder vermehrt bei mir eingegangenen Anfragen beantwortet und Beschwerden als unbegründet abgewiesen. Im Einzelfall wurde eine gerichtliche Klärung in Aussicht gestellt. Bislang ist allerdings noch kein Klagverfahren rechtshängig.

126 Wie bereits früher[51] angemerkt, lassen die vielen Eingaben rund um die Nutzungsmessung erkennen, wie wichtig es ist, dass die Rundfunkanstalten die von ihnen eingesetzten Anwendungen in ihren Datenschutzerklärungen leicht zugänglich, verständlich und transparent erläutern, wie dies die Artt. 12 ff. DSGVO fordern. Formalrechtlich können sich die Rundfunkanstalten zwar auf den Standpunkt stellen, dass sie das in den §§ 12 bzw. 23 Abs. 1 MStV verankerte „Medienprivileg" von einer dahingehenden Informationspflicht befreie. Allerdings spricht vieles dafür, dass das „Medienprivileg" auf derartige Sachverhalte nicht zugeschnitten ist. Unabhängig davon liegt es im eigenen Interesse der Rundfunkanstalten, sich nicht auf eine derart formalrechtliche Position zurückzuziehen. Nicht nur, um der Datenschutzaufsicht – und sich selbst – die Mühe der Beantwortung entsprechender Anfragen und Beschwerden zu ersparen. Sondern vor allem, um die Besonderheiten der Datenverarbeitung für die publizistischen Zwecke des öffentlich-rechtlichen Rundfunks zu vermitteln und die Akzeptanz dafür zu fördern. Auch deshalb habe ich dieser Frage bei meiner letztjährigen Prüfung besondere Aufmerksamkeit gewidmet (unten Rn. 153 ff.).

g Personalisierung und gerätebezogene Individualisierung der ZDF-Mediathek

127 Konsequenzen hatte das Inkrafttreten des TTDSG hingegen für die vom ZDF für seine Mediathek eingesetzte Individualisierungsfunktion. Im Gegensatz zur Personalisierung, der die Nutzer durch das Einrichten eines eigenen Kontos in der Mediathek ausdrücklich zustimmen und dadurch eine auf ihre spezifischen Interessen zugeschnittene Auswertung und Darstellung der Mediathek herbeiführen, ermöglicht die Individualisierung „nur" eine gerätebezogene Konfiguration des Angebots. Konkret werden dabei die entsprechenden Nutzungsdaten ohne Verwendung einer zusätzlichen ID im sogenannten local-storage-Bereich des jeweiligen Browsers bzw. bei Apps an anderer Stelle im Endgerät abgelegt. Dies betrifft insbesondere die Adresse der vom jeweiligen Nutzer aufgerufenen, gesehenen oder in die Merkliste eingetragenen bzw. mit einem Like versehenen Seiten der ZDF-Mediathek.

128 Ein Personenbezug ist damit nicht hergestellt, weil das ZDF das jeweilige Endgerät keinem bestimmten Nutzer zuordnen kann. Nach Inkrafttreten des TTDSG ist diese Datenverarbeitung jedoch dessen ungeachtet aus den oben (Rn. 19, 118) erläuterten Gründen ohne Einwilligung der Nutzer nur noch nach Maßgabe von § 25 Abs. 2 TTDSG zulässig. Deshalb müsste die mithilfe der Datenverarbeitungsvorgänge ermöglichte Individualisierungsfunktion der ZDF-Mediathek „unbedingt erforderlich" sein, damit das ZDF einen vom Nutzer „ausdrücklich gewünschten Telemediendienst" zur Verfügung stellen kann. Beide Voraussetzungen sind hier allerdings nicht erfüllt:

[51] TB 2020 Rn. 111

129 Anders als die Datenverarbeitung zur anonymisierten Nutzungsmessung dient die Individualisierungsfunktion dem ZDF nicht dazu, seine Mediathek in ihrer Gesamtheit, also „als solche“ auf einer gewissermaßen objektivierten Ebene publizistisch wettbewerbsfähig zu konfigurieren. Hier geht es vielmehr darum, dem einzelnen Nutzer den Zugang zu (möglicherweise) für ihn besonders interessanten bzw. passenden Inhalten zu erleichtern und ihn damit „in das ZDF-Angebot hinein“ zu führen bzw. ihn dort zu halten. Die individualisierte Aufbereitung der Mediathek-Inhalte stärkt die publizistische Position des ZDF also weniger objektiv bzw. unmittelbar als vielmehr auf einer individuellen, subjektiven Ebene und damit mittelbar. Gerade dies spricht aber gegen die Annahme, die Datenverarbeitung zur Individualisierung der Mediathek sei von den Nutzern „ausdrücklich gewünscht“. Denn dies liefe auf den Zirkelschluss hinaus, dass sie schon deshalb keiner Einwilligung der Nutzer bedürfe, weil sie im (hier unterstellten) publizistischen Interesse des ZDF zur Umsetzung seines Funktionsauftrags liege und deshalb (rundfunkrechtlich) zulässig sei. Die Rechtmäßigkeit des mit der Datenverarbeitung verfolgten Ziels ist aber lediglich die Prämisse und nicht etwa die Rechtfertigung für eine Ausnahme vom Grundsatz des § 25 Abs. 1 TTDSG, nach der die einschlägige Datenverarbeitung bzw. der damit verbundene Eingriff in die Privatsphäre das ausdrückliche Einverständnis der Nutzer voraussetzt. Dass das mit der Datenverarbeitung verfolgte Ziel rechtmäßig ist, bedeutet nicht, dass die Nutzer sie ausdrücklich wünschen.

130 Aus der subjektiven Perspektive kann das (ebenfalls unterstellte) Interesse der Nutzer an einer Individualisierungsfunktion nicht für sich allein dem von § 25 Abs. 2 Nr. 2 TTDSG geforderten „ausdrücklichen Wunsch“ entsprechen. Denn dieser Wunsch muss sich nach Sinn und Zweck der Vorschrift auf den Telemediendienst mit den ihm gleichsam inhärenten, funktionsnotwendigen und als solchen auch erkennbaren Merkmalen beziehen. Die Nutzer müssten also wissen, dass die ZDF-Mediathek eine Individualisierungsfunktion einsetzt, und sie müssten sie (in ihrer Gesamtheit) gerade deswegen wünschen. Dafür gibt es allerdings keinen Anhaltspunkt. Ein bloßer – wenn auch rundfunkrechtlich noch so gut begründbarer – individueller oder objektiver Nutzen allein kann dafür nicht genügen, denn § 25 TTDSG dient der Abwehr ungefragter Eingriffe in die Privatsphäre und stellt daher die subjektive Perspektive in den Vordergrund. Dass das mit der Datenverarbeitung verfolgte Ziel (subjektiv wie objektiv) nützlich ist, bedeutet also nicht, dass sie der individuelle Nutzer ausdrücklich wünscht. Anderenfalls entspräche auch dies einem Zirkelschluss und die Vorschrift liefe in allen vergleichbaren Fällen leer.

131 Unabhängig davon ist die Individualisierungsfunktion für die ZDF-Mediathek auch nicht „unbedingt erforderlich“ im Sinne von § 25 Abs. 2 Nr. 2 TTDSG. Anders als die Nutzungsmessung stärkt sie die Mediathek nicht als Gesamtangebot im publizistischen Wettbewerb, sondern „lediglich“ in ihrer konkreten Konfiguration im Verhältnis zum einzelnen Nutzer. Daraus mag sich zwar in der Summe ein objektiver Vorteil im publizistischen Wettbewerb ableiten; unbedingt erforderlich aber kann diese Funktion dafür kaum sein. Denn das Interesse des einzelnen Nutzers daran, in der Fülle der in der ZDF-Mediathek angebotenen Inhalte die für ihn interessanten und geeigneten zu finden, lässt sich außer durch eine intensivierte redaktionelle Aufbereitung bzw. Erschließung aller Inhalte (im Sinne einer „Inhalteübersicht“ o,ä.) beispielsweise auch durch eine optimierte Suchfunktion oder sonstige Erschließungshilfen bedienen.

132 Anders als im Falle der Nutzungsmessung spricht außerdem wenig für die Annahme, dass der publizistische Erfolg der Individualisierung ernsthaft gefährdet bzw. beeinträchtigt wird, wenn sie nur mit Einwilligung der Nutzer stattfindet. Trotz des in die Auslegung von § 25 Abs. 2 Nr. 2 TTDSG einzubeziehenden Gewichts der durch Art. 11 Abs. 2 GRCh, Art. 5 Abs. 1 S. GG geschützten Belange des ZDF im Verhältnis zu der durch Art. 7 GRCh geschützten Privatsphäre darf das ZDF die gerätebezogene Individualisierung seiner Mediathek daher nur mit ausdrücklicher Einwilligung der Endgerätenutzer aktivieren.

133 Das ZDF setzt deshalb seit dem Inkrafttreten des TTDSG ein entsprechendes Einwilligungstool ein und erläutert die dafür maßgeblichen Gründe in einem Einwilligungsbanner auf der Startseite. Dessen Gestaltung und Formulierung hat wiederum seither zu etlichen Anfragen und Beschwerden bei mir geführt, deren Prüfung zum Ende des Berichtszeitraums noch nicht abgeschlossen war.

h Datenschutz und Datenschutzaufsicht im journalistischen Bereich

134 Bereits im TB 2020 (Rn. 114 ff.) bin ich ausführlich auf zahlreiche Fragen eingegangen, die sich daraus ergeben, dass die §§ 12 bzw. 23 Abs. 1 S. 4 MStV die meisten Vorschriften der DSGVO für die Datenverarbeitung zu journalistischen Zwecken nicht anwendbar erklären. Fragen ergeben sich nicht zuletzt angesichts der sich massiv verändernden Rahmenbedingungen für diese Datenverarbeitung. Sie betreffen beispielsweise die Reichweite dieses sogenannten „Medienprivilegs“ hinsichtlich der unterschiedlichen Datenverarbeitungsvorgänge, das Verhältnis der unterschiedlichen Beteiligten zueinander und die damit verbundenen Fragen zur Verantwortlichkeit und zur jeweils zuständigen Datenschutzaufsicht, oder auch die Konsequenzen für die gebotenen technischen und organisatorischen Vorkehrungen zum Schutz der journalistischen Datenbestände.

135 Näher befasst habe ich mich im Berichtsjahr lediglich mit zwei Teilaspekten dieses nach meinem Eindruck bisher noch wenig beleuchteten Themenfelds: zum einen der Frage etwaiger Informationspflichten nach Art. 12 DSGVO (dazu schon oben Rn. 126 und unten Rn. 153 ff.), zum anderen die der Aufsichtszuständigkeit bei Programmkooperationen, etwa im Rahmen von Ko- oder Auftragsproduktionen, Recherchenetzwerken oder dergleichen:

136 Zu den für die journalistische Datenverarbeitung nicht geltenden Vorschriften gehören unter anderem die Art. 26 (Gemeinsame Verantwortung) und Art. 27 DSGVO (Auftragsverarbeitung). Das bedeutet, dass die Verantwortlichkeit für die Datenverarbeitung zwischen den Kooperationspartnern im Programmbereich nicht vertraglich geregelt werden muss; außerdem liegt die Aufsichtszuständigkeit jeweils bei der für den jeweiligen Kooperationspartner zuständigen Behörde. Daraus wiederum folgt, dass der Rundfunkdatenschutzbeauftragte zwar außerhalb der Datenverarbeitung für journalistische Zwecke auch etwaige Datenschutzverletzungen bei Auftragsverarbeitern der Rundfunkanstalt zu prüfen hat, nicht hingegen gegenüber Programmkooperationspartnern, weil diese nicht per se als Auftragsverarbeiter gelten. Demzufolge liegt also die Datenschutzaufsicht für den externen Dienstleister, der für die Rundfunkanstalt (oder eines ihrer Beteiligungsunternehmen) Daten zu journalistischen Zwecken verarbeitet, nicht beim Rundfunkdatenschutzbeauftragten, sondern bei dessen „originärer“ Datenschutzaufsichtsbehörde. Im Konfliktfall beurteilt

daher sie, ob und inwieweit der Vertragspartner der Rundfunkanstalt tatsächlich Daten für journalistische Zwecke verarbeitet, ob er insoweit das Datengeheimnis wahrt, und ob er die Integrität und Vertraulichkeit der Daten hinreichend gewährleistet. Dies betrifft in erster Linie Ko- und Auftragsproduzenten der Rundfunkanstalten. Aber auch sonstige Kooperationen im journalistischen Bereich wie etwa eine Zusammenarbeit mit journalistisch aktiven Organisationen oder im Rahmen eines gesellschaftsrechtlich strukturierten Recherchenetzwerks könnten insoweit betroffen sein.

137 Das mutet insofern kurios an, als die Ratio der Rundfunkdatenschutzaufsicht gerade darin liegt, dass sie qua Funktion prädestiniert dafür ist, die spezifischen Abgrenzungs- und Anwendungsfragen des Datenschutzes im journalistischen Bereich beurteilen und einordnen zu können. Daher ist fraglich, ob dem Gesetzgeber diese Konsequenz der Freistellung journalistischer Datenverarbeitung auch von diesen Vorschriften bewusst bzw. ob sie gewollt war. Zwar bleibt es den Kooperationspartnern unbenommen, freiwillig einen Auftragsverarbeitungsvertrag zu schließen und auf diese Weise – vorsorglich – darauf hinzuwirken, dass die Aufsichtszuständigkeit allein beim Rundfunkdatenschutzbeauftragten liegt. Freilich setzt dies voraus, dass den Beteiligten dieses Thema überhaupt als potentielles Problem bewusst ist. Zudem müsste der Auftraggeber bereit sein, die möglichen Nachteile eines Auftragsverarbeitungsverhältnisses dafür in Kauf zu nehmen. Vorzugswürdig wäre auf jeden Fall eine gesetzliche Klarstellung, nach der in allen derartigen Kooperationsverhältnissen die Zuständigkeit bei der Rundfunkdatenschutzaufsicht liegt.

138 Im übrigen haben mich im Berichtsjahr erneut zahlreiche Anfragen und Beschwerden unterschiedlichster Art zu Themen mit unmittelbarem oder mittelbarem Programmbezug erreicht. Im Regelfall habe ich die Absender wegen der von ihnen behaupteten Persönlichkeitsrechtsverletzungen aus den bereits früher (TB 2019 Rn. 12 ff.) erläuterten Gründen an die jeweils verantwortliche Rundfunkanstalt verwiesen.

i Beschäftigtendatenschutz

139 Wie in den Vorjahren war ich nur mit wenigen Vorgängen befasst, in denen es um Datenschutz im Beschäftigungsverhältnis ging. Erwähnt sei hier nur eine Beschwerde, deren Gegenstand der Vorwurf einer Abfrage des Impfstatus durch den Arbeitgeber war. Die betroffene Person trug vor, sie sei von ihrem Vorgesetzten mehrfach dazu gedrängt worden, ihren Impfstatus offenzulegen. In einem Fall sei sogar eine offene Namensliste im Umlauf gebracht worden, in die sich alle Beschäftigten mit den entsprechenden Angaben hätten eintragen sollen. Zwar habe der Vorgesetzte betont, dass die Teilnahme freiwillig sei. Da er das Vorgehen aber mit dem angeblichen Wunsch vieler anderer Beschäftigter begründet habe, fühlte sich die betroffene Person mindestens moralisch unter Druck gesetzt.

140 Es erwies sich als schwierig, den Sachverhalt aufzuklären, da die betroffene Person darum gebeten hatte, ihre Beschwerde anonym zu behandeln; meine entsprechende Anfrage konnte sich deshalb nicht auf den betreffenden Bereich allein beziehen. Immerhin bestätigte sich, dass Führungskräfte in einzelnen Bereichen um entsprechende Auskünfte gebeten hatten. Sowohl individuell als auch später im Intranet sei jedoch stets ausdrücklich auf die Freiwilligkeit entsprechender Angaben hingewiesen worden. Daneben sei der Impfsta-

tus einmalig im Wege einer anonymen Online-Abfrage erhoben worden, die keinerlei Rückschlüsse auf einzelne Personen zugelassen habe.

141 Daraus ergab sich, dass der Arbeitgeber es für zulässig und wohl auch geboten gehalten hatte, den Impf- oder Genesenenstatus seiner Beschäftigten auf freiwilliger Basis abzufragen. Allerdings sind die Anforderungen an eine im Rechtssinne „freiwillige" Erklärung und damit eine wirksame Einwilligung in die Datenverarbeitung im Beschäftigungsverhältnis besonders streng. Dies gilt umso mehr, wenn es sich – wie hier – um Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO handelt.

142 Letztlich musste ich die Prüfung aber nicht abschließen. Denn bevor ich den Sachverhalt vollständig aufklären konnte, hatte sich die Rechtslage geändert. Mittlerweile darf der Arbeitgeber den Zugang zum Betrieb von der Vorlage eines Impf-, Genesenen- oder Testnachweises abhängig machen. Soweit es um die Zugangsberechtigung zum Arbeitsplatz geht, erhebt der Arbeitgeber die entsprechenden personenbezogenen Daten nun also auf Basis einer ausdrücklichen gesetzlichen Grundlage und ist auf „freiwillige" Erklärungen seiner Beschäftigten nicht mehr angewiesen. Dies macht im Regelfall entsprechende individuelle Nachfragen also unzulässig. Davon unberührt bleibt nur das Recht, Beschäftigte um entsprechende Angaben zu bitten, um den möglichen Verlust des Anspruchs auf Lohnfortzahlung im Krankheitsfall zu überprüfen.

143 Im übrigen spricht das bisher geringe Anfrage- bzw. Beschwerdeaufkommen zum Beschäftigtendatenschutz dafür, dass der Schutz der personenbezogenen Daten dieser Personengruppe bei den damit befassten internen Stellen der Rundfunkanstalten und ihrer Beteiligungsgesellschaften einerseits sowie den internen Datenschutzbeauftragten andererseits in guten Händen zu liegen scheint. Möglicherweise spielt dabei aber auch eine Rolle, dass den in den Organisationen meines Zuständigkeitsbereichs Beschäftigten die Option, sich an die spezifische Rundfunkdatenschutzaufsicht zu wenden, noch nicht hinreichend bekannt ist, nachdem über Jahrzehnte hinweg in solchen Fällen (nur) der Weg zum internen Datenschutzbeauftragten zur Verfügung stand. Insoweit macht sich leider auch nachteilig bemerkbar, dass ich in den beiden zurückliegenden Jahren kaum Gelegenheiten zur Präsenz vor Ort hatte.

4 Meldungen nach Art. 33 DSGVO

144 Nach Art. 33 DSGVO ist der Verantwortliche (oder dessen 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. Dabei hat zunächst stets der Verantwortliche zu prüfen, ob die Voraussetzungen eines meldepflichtigen Vorgangs und der in den Fällen des Art. 34 DSGVO vorgeschriebenen Benachrichtigung davon betroffener Personen vorliegen. Damit trägt er auch das Risiko eines etwaigen schuldhaften Unterlassens. Ein solches kann zu aufsichtsrechtlichen Sanktionen führen. Im Zweifel sollte der Verantwortliche daher über einen Datenschutzvorfall stets die Aufsicht benachrichtigen.

145 Nicht nur in meiner, sondern auch in der Praxis der staatlichen Datenschutzbehörden zeigt sich, dass die sehr weit gefassten Vorgaben des Art. 33 DSGVO die Verantwortlichen verunsichern. Während einige vorsorglich jeden kleinsten Vorfall melden, beschränken sich andere auf offenkundig problematische Sachverhalte. Der Europäische Datenschutzausschuss (EDSA) hat daher im Dezember 2021 neue „Leitlinien" veröffentlicht[52], die am Beispiel typischer Fallkonstellationen – denen in der Regel auch die mir zugegangenen Meldungen zuzuordnen waren - Handlungs- und Verhaltenshinweise geben.

146 Darüber hinaus haben die Datenschutzbeauftragten in meinem Zuständigkeitsbereich Interesse an aufsichtsbehördlichen Kriterien gezeigt, anhand derer sie entsprechende Vorfälle besser einordnen und handhaben können. Nicht zuletzt könnte dies der Entlastung sowohl der Verantwortlichen wie auch der Aufsichtsbehörde dienen. Einschlägige Erfahrungen oder gar Vorbilder gibt es dazu allerdings weder in der DSK noch gar in der RDSK. Auch ist fraglich, inwieweit der Anwendungsbereich von Art. 33 DSGVO überhaupt durch derartige Handreichungen auf nationaler Ebene operationabel gemacht werden kann. Jedenfalls dürfte dies die Rechte bzw. Interessen potentiell betroffener Personen nicht beeinträchtigen. Intensiver befassen konnte ich mich mit diesem Thema bislang nicht.

147 Mehrere bei mir eingegangene Meldungen waren auf Fehler beim Mailversand zurückzuführen. In einem Fall lag dem ein individuell zurechenbares datenschutzwidriges Verhalten zugrunde, das zugleich gegen eine ausdrückliche interne Vorschrift verstieß. Daher stellte sich hier nach meiner Beurteilung vorrangig die Frage nach arbeitsrechtlichen und weniger die nach aufsichtsbehördlichen Konsequenzen. Auf eine Sanktion habe ich deshalb unter Verhältnismäßigkeitsgesichtspunkten verzichtet. Anders als einige staatliche Datenschutzaufsichtsbehörden und auch Stimmen in der einschlägigen Literatur bin ich nicht der Auffassung, dass jede Datenschutzverletzung zwingend mindesten mit einer Verwarnung (Art. 58 Abs. 2 lit. b DSGVO) als dem in der DSGVO vorgesehenen mildesten Mittel zu ahnden ist. Gegen diese Interpretation spricht, dass Art. 58 Abs. 2 DSGVO jeder Aufsichtsbehörde den Einsatz der dort genannten Abhilfebefugnisse „gestattet". Terminologisch impliziert dies ein Ermessen nicht nur für die Auswahl des Mittels („Wie"), sondern auch bezogen darauf, ob eine Sanktion überhaupt angezeigt ist („Ob").

148 Allerdings hielt ich in dem betreffenden Fall eine Verwarnung aus anderen Gründen für erforderlich: die Meldung war mir deutlich jenseits der von Art. 33 DSGVO vorgegebenen Regelfrist von 72 Stunden zugegangen. Sie hat der Verantwortliche zwar nur „möglichst" einzuhalten. Ob er das ihm mögliche unternommen hat, hängt stets von einer Einzelfallbetrachtung ab. Mehrere – hier: neun - Tage nach Ablauf der Regelfrist kann eine Meldung freilich nur in einem besonders gelagerten Einzelfall noch fristgerecht sein, den der Verantwortliche dann auch explizit zu erläutern hat, Art. 33 Abs. 1 S. 2 DSGVO. Wie nicht zuletzt EG 85 und die Bußgeldvorschriften der DSGVO (Art. 83 Abs. 4 lit. a: Geldbuße bis zu 10 Mio. Euro) erkennen lassen, haben die Meldeverpflichtungen durchaus hohes Gewicht. Der Verantwortliche muss daher im eigenen Interesse durch geeignete organisatorische Vorkehrungen sowie die Sensibilisierung der Beschäftigten gewährleisten, dass Datenschutzvorfälle schnellstmöglich erkannt, bewertet und – sofern die entsprechenden Vor-

[52] EDSA (2021). Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, V 2.0.

aussetzungen vorliegen – der zuständigen Aufsichtsbehörde gemeldet werden können. Denn er trägt das Risiko einer verspäteten oder gar unterlassenen Meldung, und zumindest im Wiederholungsfall sind spürbare aufsichtsbehördliche Konsequenzen unausweichlich.

5 Auftragsverarbeitung

149 Anlass für aufsichtsbehördliche Untersuchungen oder Maßnahmen in Bezug auf Auftragsverarbeiter der Verantwortlichen in meinem Zuständigkeitsbereich gab es im Berichtsjahr nicht. In den bereits (oben Rn. 97 ff.) angesprochenen Fällen, in denen explizit die Beauftragung von Inkassounternehmen durch den Beitragsservice problematisiert worden war, ergaben sich keine Hinweise auf mögliche Verstöße des Auftragsverarbeiters gegen die ihm obliegenden datenschutzrechtlichen Verpflichtungen.

6 Kontrollen und Prüfungen

150 Gemäß Art. 51 Abs 1 und Art. 58 Abs. 1 lit. b) DSGVO hat der Rundfunkdatenschutzbeauftragte die Umsetzung der DSGVO bei den Verantwortlichen zu überwachen und zu prüfen. Dies muss nicht immer auf einen Anlass, bspw. eine Beschwerde zurückgehen, sondern kann auch in Form geplanter Audits stattfinden. Grundsätzlich habe ich eine jährliche Prüfung bei einer oder mehreren Organisationen in meinem Zuständigkeitsbereich zu einem bestimmten Schwerpunktthema vorgesehen, über das ich die Verantwortlichen jeweils rechtzeitig vorher informiere.

151 Im Vorjahr hatte ich überprüft, inwieweit die Rundfunkanstalten ein den Anforderungen des Art. 30 DSGVO entsprechendes **Verzeichnis ihrer Verarbeitungstätigkeiten** führen (s. dazu ausführlich TB 2020 Rn. 137 ff.). In allen Fällen ergab die Prüfung Defizite in unterschiedlichem Ausmaß, teils auch in struktureller Hinsicht, soweit es etwa um die von mehreren oder allen Rundfunkanstalten gemeinsam verantworteten Einrichtungen ging. Bis Ende Mai 2021 informierten mich die Verantwortlichen über die von ihnen daraufhin ergriffenen oder zumindest veranlassten Maßnahmen. Einen vollständig DSGVO-konformen Zustand versicherten mir bis Ende des Jahres die meisten, aber noch nicht alle Rundfunkanstalten. Ich habe eine gelegentliche Nachprüfung angekündigt.

152 Gegenstand meines Audits im Berichtsjahr war die stichprobenartige Überprüfung von insgesamt 24 **Datenschutzerklärungen (DSE)** von Rundfunkanstalten bzw. deren Gemeinschaftseinrichtungen sowie Beteiligungsunternehmen in meinem Zuständigkeitsbereich. Jeweils acht der 24 DSE gehören zu Websites bzw. Apps von Rundfunkanstalten oder ihren Gemeinschaftseinrichtungen sowie zu Websites von Beteiligungsgesellschaften. Festzustellen war, ob und inwieweit die betreffenden DSE die in den Artt. 12 und 13 DSGVO festgelegten Informations- und Transparenzpflichten erfüllen, insbesondere die nach diesen Vorschriften geforderten Informationen transparent sowie vollständig und richtig darstellen. Wie im Vorjahr ging es darum, die Verantwortlichen auf den dabei zutage getrete-

nen Handlungsbedarf sowie Optimierungsmöglichkeiten bei der Gestaltung und Formulierung ihrer DSE aufmerksam zu machen.

153 Für diesen Prüfgegenstand habe ich mich entschieden, weil die Informations- und Transparenzpflichten nach Artt. 12 ff. DSGVO, ähnlich wie die Vorgaben des Art. 30 DSGVO zum Verzeichnis der Verarbeitungstätigkeiten, sowohl nach innen wie auch nach außen wirken: Zwar dient die DSE in erster Linie dazu, die von der Verarbeitung ihrer personenbezogenen Daten Betroffenen zu informieren und zu sensibilisieren. Im Sinne einer „Visitenkarte" vermittelt sie insoweit einen Eindruck vom Stellenwert, den der Verantwortliche dem Datenschutz bzw. seinen Informations- und Transparenzpflichten beimisst. Zugleich ist die DSE für den Verantwortlichen selbst aber auch ein Instrument der Vergewisserung darüber, ob die von ihm veranlasste Datenverarbeitung alle gesetzlichen Anforderungen erfüllt. In praktischer Hinsicht hatte dieses Prüfthema den Vorteil, dass ich weder auf interne Unterlagen noch auf Untersuchungen und Gespräche vor Ort angewiesen und deshalb von pandemiebedingten Unwägbarkeiten unabhängig war.

154 Die teilweise sperrige Datenschutzmaterie mit ihren vielen rechtlichen Bezügen verständlich zu erläutern, ist gewiss kein leichtes Unterfangen und nicht ohne einigen Aufwand zu bewerkstelligen. Dies konstatieren nicht zuletzt einschlägige Berichte der Rundfunkanstalten selbst, die sich mit diesem Thema befassen. So stellt etwa der BR im Juni 2019 mithilfe des „Regensburger Analysetools für Texte" fest, dass typische Datenschutzerklärungen im Schnitt 8,4 komplizierte Wörter aufweisen, während etwa Thomas Mann in seiner Novelle „Der Tod in Venedig" nur 5 verwendet habe[53].

155 Ob ein solcher Beurteilungsmaßstab sinnvoll oder auch nur tauglich ist, mag hier dahinstehen. In jedem Fall sollte eine DSE für jede durchschnittliche, nicht rechtlich ausgebildete Person ohne größere Mühe verständlich sein. Dies ist jedenfalls die Perspektive, die der Prüfung zugrunde liegt. Sie orientiert sich außerdem an einem Grundverständnis, nach dem der öffentlich-rechtliche Rundfunk in besonderer Weise aufgefordert ist, sein Publikum über die datenschutzrechtlichen Konsequenzen seiner Aktivitäten im Onlinebereich verständlich und vollständig aufzuklären (s. dazu bereits TB 2020 Rn. 111).

156 Immer wieder bei mir eingehende Anfragen und Beschwerden belegen, dass es bei den Nutzern der öffentlich-rechtlichen Telemedienangebote – verständlicherweise - eine dahingehende Erwartungshaltung gibt. Sie speist sich aus mehreren Faktoren:

- Verlässliche, objektive, umfassende und sorgfältige Information ist der Wesenskern des öffentlich-rechtlichen Rundfunks und steht im Mittelpunkt seines verfassungsrechtlichen Funktionsauftrags. Formal betrachtet gilt das zwar nur für seine Berichterstattung. Aber mittelbar strahlt dieses Verständnis auch auf seine sonstigen Aktivitäten aus: wenn der öffentlich-rechtliche Rundfunk gehalten ist, über das allgemeine Geschehen verlässlich, objektiv, umfassend und vollständig zu informieren, erwartet die Allgemeinheit dies erst recht, wenn er die ihm selbst obliegenden Informationspflichten (hier: nach Artt. 12 ff. DSGVO) zu erfüllen hat.

[53] Harlan, Elisa; Richt, Maximilian; Schnuck, Oliver (2019, 11. Juni). Komplizierte Datenschutzerklärungen: Der Haken am Häkchen, Projekt von BR Recherche und BR Data. https://interaktiv.br.de/datenschutzerklaerungen [Stand: 25.02.2022].

- Die Allgemeinheit finanziert den öffentlich-rechtlichen Rundfunk durch den Rundfunkbeitrag. Sie will daher die Nutzung seiner Onlineangebote nicht (zusätzlich) damit „bezahlen", dass die Rundfunkanstalten oder Dritte ihre personenbezogenen Daten verarbeiten, ohne dass sie darüber informiert sind und dies gegebenenfalls unterbinden können.
- Im engen Zusammenhang mit den beiden erstgenannten Aspekten steht ein dritter: große Teile seines Publikums nehmen den öffentlich-rechtlichen Rundfunk als Sachwalter ihrer Interessen wahr. Sie schreiben ihm daher eine „Vorbildfunktion" zu, die sich signifikant unterscheidet von den Gepflogenheiten anderer Akteure im Internet, namentlich der kommerziellen „Datenkraken".
- Und schließlich ist der öffentlich-rechtliche Rundfunk verpflichtet, die gesamte Bevölkerung zu erreichen: Mit seinen Angeboten, aber – gerade deshalb - auch mit seinen Informationen in eigener Sache. Diese müssen also so niederschwellig wie möglich erreichbar und für die Allgemeinheit ohne Vorkenntnisse verständlich formuliert sein.

157 Daraus folgt: Im Idealfall sollte der öffentlich-rechtliche Rundfunk (und dies schließt seine Beteiligungsunternehmen ein) mit den von ihm verantworteten DSE den Standard setzen und sich nicht darauf beschränken, nur Mindestanforderungen zu erfüllen. Allerdings kann ich dies aufsichtsbehördlich weit überwiegend nur empfehlen, nicht hingegen konkret vorgeben. Denn formalrechtlich gewähren die Vorschriften der Artt. 12 ff. DSGVO dem Verantwortlichen einen beträchtlichen Spielraum zur Formulierung und Gestaltung seiner DSE. Nur punktuell ergeben sich aus ihnen unmittelbar ableitbare konkrete Vorgaben. Und gerade in Bezug auf die Datenverarbeitung zur Nutzungsmessung, die in der Praxis die meisten Anfragen und Beschwerden auslöst, lässt sich sogar die Auffassung vertreten, dass die §§ 12 bzw. 23 Abs. 1 MStV die Rundfunkanstalten von der Informationspflicht gleich ganz befreien, dient sie doch journalistischen Zwecken. Mit Blick auf die hier erläuterte grundsätzliche Einordnung der gesetzlichen Verpflichtungen habe ich jedoch auch in Bezug auf die interpretations- und ausgestaltungsfähigen Vorgaben der Informations- und Transparenzregelungen bewusst den hier umrissenen hohen Anspruch zugrunde gelegt.

158 Grundlage der Prüfung war eine Checkliste in Gestalt einer adaptierten Kurzfassung der „Leitlinien für Transparenz" des EDSA[54]. Sie ist diesem TB ebenso als Anlage beigefügt wie die Übersicht über die Ergebnisse der Prüfung aller 24 DSE. Danach weisen alle untersuchten DSE in unterschiedlichem Umfang Verbesserungspotenzial auf und entsprechen in einigen Punkten nicht vollständig den gesetzlichen Vorgaben. Die farbliche Grundierung der einzelnen Punkte in der Gesamtübersicht soll in erster Linie einen raschen Überblick über das Ergebnis des Soll-/Ist-Abgleichs ermöglichen. Prüfungs- bzw. Handlungsbedarf im engeren Sinne besteht nur in den rot gekennzeichneten Punkten, wobei er sich insoweit nicht notwendig auf das dort jeweils bezeichnete Thema insgesamt erstreckt, sondern in der Regel auf Detailaspekte beschränkt. Jedem Verantwortlichen habe ich darüber hinaus eine Detailauswertung der jeweiligen DSE mit kurzen Begründungen sowie Hinweisen auf Formulierungsbeispiele zur Verfügung gestellt.

[54] Artikel-29-Datenschutzgruppe (2018). Guidelines on transparency under Regulation 2016/679, WP 260 rev. 0.1 in der Fassung vom 11. April 2018.

159 Hervorzuheben ist, dass keine der untersuchten DSE die erforderlichen Informationen zu den erhobenen Daten, den Zwecken der Verarbeitung und deren Rechtsgrundlagen vollständig enthält. Auffällig ist außerdem, dass die DSE von Apps in den meisten Fällen nicht eigens für die Verarbeitung von personenbezogenen Daten innerhalb der Apps formuliert sind. Stattdessen wird die DSE der jeweiligen Website (oder ein Ausschnitt daraus) verwendet, ohne den Text adäquat anzupassen. Dadurch sind die Anforderungen an die Transparenz der Information besonders häufig nicht erfüllt, und Angaben zu Verarbeitungsvorgängen fehlen.

160 Etliche Datenverarbeitungsvorgänge bzw. Sachverhalte, über die die DSE informieren muss, treten bei allen Rundfunkanstalten und ihren Gemeinschaftsprogrammen weitgehend oder vollständig identisch auf, werden dort aber teilweise sehr unterschiedlich dargestellt. Das ist aus Nutzersicht verwirrend und macht sich vor allem dort nachteilig bemerkbar, wo es um Sachverhalte geht, die für das Verständnis der Nutzer über den Datenschutz im öffentlich-rechtlichen Rundfunk besonders bedeutsam sind. Ich habe deshalb empfohlen, mindestens für die folgenden Themen einheitliche Textbausteine zu formulieren und in die DSE aller Rundfunkanstalten und ihrer Gemeinschaftsprogramme zu integrieren:

- Erläuterung technischer und juristischer Fachbegriffe in einem Index
- DSE für Kinder und Jugendliche
- Information über die Datenverarbeitung zur Nutzungsmessung einschließlich vollständiger Angaben zum berechtigten Interesse und zur Anonymisierung
- Information zum Medienprivileg
- Betroffenenrechte

161 Selbstverständlich sind die Rundfunkanstalten frei darin, ob sie diesen Empfehlungen folgen. Sie könnten ihre Datenschutzerklärungen aber auch noch weitergehend einander angleichen. Es wäre ein erfreuliches Zeichen von Datenschutz- und Nutzerfreundlichkeit, wenn die Gestaltung, die Systematik und der Inhalt der Datenschutzinformationen im öffentlich-rechtlichen Rundfunk sich weitgehend in einem einheitlichen Rahmen bewegte. Nicht zuletzt würde dies den Aufwand auf Seiten aller Beteiligten – der Rundfunkanstalten selbst, der Nutzer und der Datenschutzaufsicht – reduzieren.

162 **Vor-Ort-Kontrollen** habe ich im Berichtsjahr angesichts der weiterhin stark eingeschränkten Präsenzmöglichkeiten nicht durchgeführt.

7 Zahlen und Fakten 2021

163 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. Angesichts ihrer relativ geringen Aussagekraft und mit Blick auf vorrangige Aufgaben verzichte ich auf eine derartige Liste. Zu den entsprechenden Anlässen und Reaktionen habe ich mich bereits im unmittelbaren Zusammenhang mit dem jeweiligen Thema geäußert. Stattdessen sind im folgenden einige aggregierte Kenndaten meiner Tätigkeit im Berichtsjahr dargestellt.

164 Im Jahr 2021 haben mich erneut insgesamt rund 200 Zuschriften erreicht, mit denen sich außenstehende Dritte an mich gewandt haben. Berücksichtigt sind hierbei nur die durch externe Eingaben veranlassten Korrespondenz- bzw. Aufsichtsvorgänge, nicht hingegen die Beratungs- und Konsultationsanfragen im Verhältnis zu den Verantwortlichen bzw. ihren Datenschutzbeauftragten in meinem Zuständigkeitsbereich. Ebenfalls nicht statistisch erfasst sind die teilweise sehr aufwändigen Prüfvorgänge, mit denen ich in anderen Zusammenhängen befasst war.

165 Die weit überwiegende Zahl der Eingaben erreicht mich per Mail oder über das auf meiner Website angebotene Kontaktformular, ein weiter abnehmender kleiner Teil auf dem Postweg. Auch 2021 ist im Verlauf der Corona-Pandemie – ein wenig überraschend – das Beschwerdeaufkommen weiter zurückgegangen. Durchschnittlich haben mich monatlich etwa 16 Eingaben erreicht.

a Beschwerde

166 Mit einer Beschwerde reklamiert die betroffene Person, selbst von einer Datenschutzverletzung betroffen zu sein. Insgesamt gingen mir über 90 förmliche Beschwerden zu. Etwa die Hälfte von ihnen betraf den Beitragsservice von ARD, ZDF und Deutschlandradio. 23 Beschwerden richteten sich gegen das ZDF oder eines der von ihm verantworteten Gemeinschaftsprogramme (3sat, Phoenix), 14 gegen den WDR, 7 gegen den BR, jeweils eine gegen den SR und das Deutschlandradio. Insgesamt drei Beschwerden erwiesen sich zumindest teilweise als begründet, alle anderen habe ich nach Prüfung als unbegründet abgewiesen.

b Anzeige

167 Gelegentlich reklamiert eine Person eine vermeintliche Datenschutzverletzung, die (im Gegensatz zur Beschwerde) nicht unmittelbar sie selbst, sondern andere betrifft. Außerdem sind unter dieser Rubrik anonyme Hinweise auf (vermeintliche) Datenschutzverstöße subsumiert, die mich beispielsweise über mein Online-Meldeformular oder über den Bundes- bzw. einen Landesbeauftragten für Datenschutz und Informationsfreiheit erreicht haben.

168 Die Grenzen zur Beratungsanfrage (siehe c) sind hier fließend; außerdem betreffen derartige Eingaben häufig (vermeintliche) Datenschutzverstöße in Sendungen der Rundfunkanstalten. Zu vier dieser Anzeigen habe ich ausführlich Stellung genommen.

c Beratungsanfrage

169 Der RDSB hat als Aufsichtsbehörde in erster Linie die rechtlich geschützten Interessen jener zu vertreten, die (potentiell) von einer Verarbeitung der auf sie bezogenen Daten in seinem Zuständigkeitsbereich betroffen sind. Dies umfasst auch eine allgemeine Beratung

zu Fragen zum Datenschutz und zur Datenverarbeitung bei den Verantwortlichen oder durch meine Aufsichtsbehörde selbst (Beratungsanfrage). Die meisten der insgesamt 15 entsprechenden Eingaben habe ich inhaltlich beantwortet und die Rechtslage erläutert; die restlichen waren aus formellen Gründen an andere Stellen zu verweisen.

170 Nicht hier, sondern unter h) gesondert erfasst sind alle Beratungsvorgänge im Verhältnis zu den Verantwortlichen in meinem Zuständigkeitsbereich.

d Datenschutz im Programm

171 Dass die Datenverarbeitung zu journalistischen Zwecken weder den allgemeinen Datenschutzbestimmungen noch der Datenschutzaufsicht unterliegt, ist vielfach nicht hinreichend bekannt. Auch im Berichtsjahr erreichten mich dazu vierzehn konkrete Eingaben. Zu sechs von ihnen habe ich jeweils ausführlich Stellung genommen und die Rechtslage erläutert.

e Auskunftsersuchen nach Art. 15 DSGVO

172 Auch meine Aufsichtsbehörde verarbeitet personenbezogene Daten. Sie ist insoweit selbst Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Daher ist sie auf entsprechenden Antrag hin zur Auskunft gemäß Art. 15 DSGVO verpflichtet. Allerdings umfasst dieser Anspruch nur die unmittelbar in der Aufsichtsbehörde selbst verarbeiteten Daten und nicht etwa (auch) jene, die die anderen Verantwortlichen in meinem Zuständigkeitsbereich verarbeiten. Das Gros der entsprechenden Eingaben bezog sich jedoch auf den ZBS oder eine der Rundfunkanstalten, die die Anspruchsteller durch mich vertreten glaubten und an die ich sie daher verwiesen habe.

173 Zwölf Auskunftsbegehren gemäß Art. 15 Abs. 1 DSGVO richteten sich direkt oder inzident an mich als Aufsichtsbehörde. In keinem dieser Fälle hatten wir bereits personenbezogene Daten zu der jeweiligen Person verarbeitet. Alle Auskunftsbegehren habe ich fristgerecht beantwortet.

f Sonstiges

174 Als eine der Aufsichtsbehörden für den Zentralen Beitragsservice wird der Rundfunkdatenschutzbeauftragte häufig in Bezug auf Kontenklärungen und Beschwerden bezüglich des Rundfunkbeitrags angeschrieben. Grund dafür ist die irrige Annahme, es handele sich um eine allgemeine Fachaufsicht. In diesen Fällen verweise ich die Petenten in der Regel an die Kontaktstellen der Rundfunkanstalten und des ZBS. Dies traf auf rund 50 Eingänge bei mir zu.

175 Nur in wenigen Fällen, in denen mindestens vordergründig ein datenschutzrechtlicher Kontext feststellbar war, habe ich mit einer inhaltlichen Stellungnahme reagiert. Zu Eingaben ohne jeden oder hinreichend konkreten Datenschutzbezug hingegen, von denen mich wei-

terhin mehrere monatlich erreichen, äußere ich mich generell nicht inhaltlich, selbst wenn dies nach erstem Anschein mit keinem größeren Aufwand verbunden wäre. Denn ich sehe es für unabdingbar an, jeden Anschein zu vermeiden, der Rundfunkdatenschutzbeauftragte sei als rundfunkspezifische Datenschutzaufsichtsbehörde letztlich doch integraler Teil der Administration der Rundfunkanstalten oder des Beitragsservice. Daher biete ich selbst die bloße Weiterleitung nicht-datenschutzrelevanter Eingaben an die Rundfunkanstalten nur in besonders gelagerten Ausnahmefällen an. Mir ist bewusst, dass die betreffenden Personen oder Organisationen dies unter Umständen als übertrieben – oder typisch - bürokratisch wahrnehmen können. Daher bemühe ich mich in solchen Fällen stets, ihnen meine Entscheidung verständlich zu erläutern und konkrete Kontaktoptionen für ihr Anliegen aufzuzeigen.

176 Auch zahlreiche Eingaben ohne jeden oder hinreichend konkreten Datenschutzbezug haben mich erreicht. Soweit möglich, habe ich die Absender an die zuständige Stelle verwiesen.

177 Im übrigen gebe ich im allgemeinen jeden Vorgang, in dem erkennbar erstmals ein allgemeines oder spezifisches datenschutzrechtliches Anliegen formuliert wird, an den Datenschutzbeauftragten des jeweiligen Verantwortlichen ab. Für allgemeine datenschutzrechtliche Erläuterungen zur Praxis der Rundfunkanstalten sehe ich die Datenschutzaufsicht nur in zweiter Linie gefragt. Entsprechendes gilt für Anliegen, die eine andere Einrichtung in meinem Zuständigkeitsbereich betreffen. Davon habe ich 2021 mehrfach Gebrauch gemacht.

178 Des weiteren sind bei mir vier Anfragen bzw. **Auskunftsersuchen nach dem Informationsfreiheitsrecht** eingegangen. In allen Fällen stützten sich die Antragsteller dabei auf ein Standardformular der Website „Frag den Staat“ und machten mit unterschiedlicher Zielsetzung Ansprüche auf Auskunft und Information sowie Überlassung von Unterlagen gegen mich geltend. Sie beriefen sich dabei auf die Vorschriften des Informationsfreiheitsgesetzes (IFG), des Umweltinformationsgesetzes (UIG) sowie des Gesetzes zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (VIG). Allerdings sind die betreffenden Bundesgesetze auf meine rundfunkspezifische Datenschutzaufsichtsbehörde gar nicht anwendbar. Abgesehen davon gingen die Ansprüche auch deshalb ins Leere, weil sie sich weder auf ein Umwelt- noch ein gesundheitsbezogenes Anliegen bezogen.

g Datenschutzvorfall

179 Eine Verletzung der Datenschutzvorgaben ist hier als Datenschutzvorfall bezeichnet. Ein solcher muss nach Art. 33 DSGVO durch die verantwortliche Stelle selbst oder deren Auftragsverarbeiter gemeldet werden und ist stets mit der Prüfung verbunden, ob und inwieweit die betroffenen Personen über eine damit verbundene Gefährdung ihrer personenbezogenen Daten zu informieren sind, Art. 34 DSGVO (s. oben Rn. 144).

180 2021 wurden mir 10 Datenschutzvorfälle gemeldet, für die ich unmittelbar zuständig war. Davon betrafen vier das ZDF, drei den WDR, zwei den BR sowie jeweils einer die Bavaria Film und die SportA. Überwiegend hatten die Verantwortlichen dafür auf das von mir auf

der Homepage zur Verfügung gestellte Meldeformular zurückgegriffen, das auf alle anzeigepflichtigen Informationen hinweist. Mit einer Ausnahme ging die Meldung innerhalb der von Art. 33 DSGVO vorgegebenen Frist bei mir ein und enthielt auch die für eine rasche aufsichtsbehördliche Bewertung erforderlichen Angaben.

h Beratung der Verantwortlichen

181 Die Beratungsfunktion des RDSB beschränkt sich sowohl nach der Logik der Rollenverteilung (Art. 39 DSGVO einerseits, Art. 57 DSGVO andererseits) als auch unter Kapazitätsgesichtspunkten gegenüber den Verantwortlichen bzw. ihren Datenschutzbeauftragten auf Angelegenheiten mit grundsätzlichem Charakter. Diese haben sich auch 2021 in unterschiedlicher Weise – allerdings in etwas geringerem Umfang als im Vorjahr - mit der Bitte um Beratung an mich gewandt. Überwiegend ging es um die Bewertung eines Vorhabens einer der Rundfunkanstalten oder des Beitragsservice, mehrfach auch um Anfragen von Beteiligungsunternehmen – bzw. in einem Fall von dessen Gesamtbetriebsrat -, unter anderem zur Vergewisserung über die Aufsichtszuständigkeit.

i Gerichtsverfahren

182 Im Berichtszeitraum war eine Klage gegen einen von mir erlassenen Bescheid vor dem örtlich für meine Behörde zuständigen Verwaltungsgericht Potsdam anhängig. Ich rechne mit einer Entscheidung im Jahr 2022.

Anlagen (zu Abschnitt 6, Rn. 152 ff.)

- Anlage 1: Checkliste Datenschutzerklärung Websites und Apps
- Anlage 2: Auswertungsübersicht Datenschutzerklärungen Websites und Apps

Anlage 1:
Checkliste Datenschutzerklärung Websites und Apps

1. **Transparenz** (Art. 12 Abs. 1 S. 1 DSGVO)
   Auffindbarkeit, Verständlichkeit

1.1. leicht zugänglich
Platzierung und Verständlichkeit des Links zur Datenschutzerklärung (für technisch und rechtlich unbedarfte, durchschnittlich informierte Nutzer ohne weiteres identifizier- und auffindbar); Erreichbarkeit von allen Seiten aus.

1.2. präzise
Genau und griffig beschrieben / keine überflüssigen, ablenkenden Inhalte / DSE speziell für Website bzw. App.

1.3. transparent
Vor oder spätestens gleichzeitig mit der erstmaligen Datenerhebung / getrennt von sonstigen Informationen, die sich nicht auf Datenschutz beziehen.

1.4. verständlich (klare und einfache Sprache)
In deutscher Sprache / möglichst wenig Substantive und technische oder rechtliche Fachbegriffe / aktive statt passiver Formulierungen / keine mehrdeutigen und unbestimmten Aussagen (Konjunktiv, Modalverben).

1.5. schriftlich, ggf. elektronisch
Einheitliches Dokument, verständliche, konsistente Gliederung (durch Inhaltsverzeichnis, Mehrebenen-DSE, Einsatz elektronischer Hilfsmittel (Bildsymbole, Verlinkungen o. ä.)) / Konsistenz von jeweiliger Überschrift und Inhalt / Maschinenlesbarkeit.

1.6. besondere Schutzgruppen (Kinder, behinderte Personen)
Kindgerechte Gestaltung und Darstellungsformen / Barrierefreiheit (einfache Sprache, ausreichender Kontrast zwischen Vorder- und Hintergrundfarbe, (verstellbare) Schriftgröße und Größe der Bedienelemente, Alternativtexte für Bilder und Symbole, Strukturelemente, Screenreader-Tauglichkeit).

2. **Inhaltliche Angaben, Art. 13 DSGVO**
   Vollständigkeit und Richtigkeit der geforderten Angaben

2.1. Verantwortliche (Art. 13 Abs. 1 lit. a DSGVO)
Kontaktdaten

2.2. Datenschutzbeauftragte (Art. 13 Abs. 1 lit. b DSGVO)
Kontaktdaten

2.3. Datenverarbeitungsvorgänge

Information über jede beim Betrieb der Website tatsächlich stattfindende DV und dabei verarbeitete personenbezogene Daten

2.3.1. Sicherheitsanalyse
2.3.2. Funktion der App
2.3.3. Nutzungsmessung
2.3.4. Individualisierung
2.3.5. Nutzerkonten
2.3.6. Kontakt (Kontaktformular, E-Mail-Kontakt)
2.3.7. Newsletter
2.3.8. Plugins
2.3.9. Drittplattformen
2.3.10. Kommentare
2.3.11. Bewerbungsverfahren
2.3.12. Sonstige

Zusätzliche Anforderungen an Apps

2.3.13. Herunterladen
2.3.14. Push-Benachrichtigungen
2.3.15. Berechtigungen
2.3.16. Offline-Betrieb

2.4. Erhobene Daten

Beschreibung der für die jeweilige Datenverarbeitungstätigkeit erhobenen und verarbeiteten Daten.

2.5. Zwecke jeder Datenverarbeitung (Art. 13 Abs. 1 lit. c DSGVO)

Angabe aller Zwecke, für die personenbezogene Daten erhoben werden / Beschreibung, aus der hervorgeht, dass eine Korrelation zwischen Datenverarbeitung und verfolgtem Zweck besteht.

2.6. Einschlägige Rechtsgrundlage jeder Datenverarbeitung (Art. 13 Abs. 1 lit. c DSGVO)

Jeweilige Rechtsgrundlage für jede Datenverarbeitung hinreichend konkret angegeben und so erläutert, dass die betroffene Person den Sachverhalt subsumieren kann.

2.7. Ggf. Erläuterung des berechtigten Interesses (Art. 13 Abs. 1 lit. d DSGVO)

Interessenabwägung (im Fall von Art. 6 Abs. 1 lit. d DSGVO): berechtigte Interessen des Verantwortlichen hinreichend konkret benannt.

2.8. Empfänger oder Kategorien von Empfängern personenbezogener Daten (Art. 13 Abs. 2 lit. a DSGVO)

Datenempfänger jenseits des Verantwortlichen, also auch Auftragsverarbeiter und gemeinsam Verantwortliche / Empfängerkategorien nur, wenn das nicht möglich bzw. zu aufwändig ist; in diesem Fall möglichst konkrete Beschreibung.

2.9. Absicht der Übermittlung in Drittland (Art. 13 Abs. 1 lit. f DSGVO)
Wenn Absicht, dann Information obligatorisch / Betr. muss Übermittlungsrisiko beurteilen können.

2.10. Speicherdauer oder Kriterien für deren Festlegung (Art. 13 Abs. 2 lit. a DSGVO)
Beginn und Dauer sowie Umfang der Speicherung, bezogen auf den jeweiligen Datenverarbeitungsvorgang.

2.11. Betroffenenrechte (Art. 13 Abs. 2 lit. b DSGVO)
Leicht auffindbarer und verständlicher Hinweis auf die einzelnen Rechte / Erklärung der angemessenen Modalitäten, diese Rechte tatsächlich auszuüben.

2.12. Widerrufsmöglichkeit (Art. 13 Abs. 2 lit. c DSGVO)
Hinweis darauf, dass und wie die betroffene Person ihre Einwilligung zurückziehen kann (im Fall von Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO).

2.13. Beschwerderecht (Art. 13 Abs. 2 lit. d DSGVO)
Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde / fakultativ, aber zu empfehlen: konkrete Benennung RDSB.

3. Bearbeitungsstand, Information über Änderungen

Angabe des Stands der aktuellen Version der DSE / dauerhafter Zugang zu allen relevanten Informationen; Information über Veränderungen, die sich auf die betroffene Person auswirken.

	br.de	daserste.de	dradio.de	3sat.de	phoenix.de	sr.de	wdr.de	zdf.de
1.1 Transparente Information								
1.1 leicht zugänglich	(✓)	(✓)	✓	✓	(✓)	(✓)	✓	✓
1.2 präzise	(✓)	(✓)	✓	✓	✓	(✓)	✓	(✓)
1.3 transparent	✓	(✓)	✓	(✓)	✓	✓	✓	✓
1.4 verständlich	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	✓	(✓)
1.5 schriftlich	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
1.6 bes. Schutzgruppen	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2. Vollständige und richtige Angaben								
2.1 Verantwort-licher	✓	(✓)	✓	(✓)	✓	✓	(✓)	(✓)
2.2 ggf. DSB	✓	✓	✓	✓	✓	✓	✓	✓
2.3 Datenverarbeitungsvorgänge								
2.3.1 Sicherheitsanalyse	✓	X	✓	✓	✓		X	✓
2.3.2 Funktion der Website		X			(✓)	(✓)	X	
2.3.3 Nutzungsmessung	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)

2.3.4 Individualisierung	X	X		X		X		X
2.3.5 Nutzerkonten	✓							✓
2.3.6 Kontakt	X	(✓)	X	✓	✓	X	X	✓
2.3.7 Newsletter	(✓)	X	(✓)		✓	X	(✓)	✓
2.3.8 Plugins	X	(✓)	(✓)		(✓)	(✓)	X	(✓)
2.3.9 Drittplattformen	X	(✓)	X	X		(✓)	X	(✓)
2.3.10 Kommentare	X	X				X	X	
2.3.11 Bewerbungsverfahren	(✓)					✓		
2.3.12 Sonstige	X	(✓)	X			X		✓
	X	(✓)	X			X		✓
		X	X			(✓)		✓
		(✓)	X					✓
2.4 Daten	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2.5 Zwecke	X	X	X	(✓)	(✓)	X	(✓)	(✓)
2.6 Rechtsgrundlage	X	X	X	X	X	X	X	X

2.7 Berechtigtes Interesse	(✓)	(✓)	X	X	X	(✓)	(✓)	X
2.8 Empfänger	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2.9 Übermittlung in Drittland	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	✓	(✓)
2.10 Speicherdauer	X	X	(✓)	(✓)	X	(✓)	(✓)	(✓)
2.11 Betroffenenrechte	(✓)	X	(✓)	(✓)	(✓)	(✓)	X	(✓)
2.12 ggf. Widerrufsmögl.	✓	(✓)	(✓)	(✓)	✓	(✓)	(✓)	✓
2.13 Beschwerderecht	(✓)	(✓)	✓	✓	✓	(✓)	✓	✓
3. Bearbeitungsstand, Information über Änderungen								
	✓	(✓)	(✓)	(✓)	(✓)	(✓)	✓	(✓)
Grundlage der Untersuchung ist die Version vom:	14.12.2021	27.07.2021	15.12.2021	30.08.2021	23.11.2021	27.08.2021	25.08.2021	26.11.2021

✓	Vorgaben vollständig umgesetzt
(✓)	Verbesserungsmöglichkeiten
(✓)	Verbesserungsbedarf
X	Rechtliche Vorgaben nicht umgesetzt
	Prüfungs- oder Ergänzungsbedarf
	Keine Datenverarbeitung / Angabe

	ard-werbung.de	ard-zdf-medien-akademie.de	br-media.de	dra.de	network-movie.de	werbe-funk-saar.de	zdf-service.de	pensions-kasse-rundfunk.de
1. Transparente Information								
1.1 leicht zugänglich	✓	✓	(✓)	✓	(✓)	(✓)	(✓)	✓
1.2 präzise	(✓)	(✓)	(✓)	✓	(✓)	✓	(✓)	(✓)
1.3 transparent	✓	✓	✓	✓	✓	✓	✓	✓
1.4 verständlich	(✓)	(✓)	(✓)	✓	(✓)	(✓)	(✓)	(✓)
1.5 schriftlich	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
1.6 bes. Schutzgruppen	✓	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2. Vollständige und richtige Angaben								
2.1 Verantwortlicher	(✓)	✓	✓	(✓)	✓	(✓)	✓	✓
2.2 ggf. DSB	✓	✓	(✓)	(✓)	✓	(✓)	(✓)	✓
2.3 Datenverarbeitungsvorgänge								
2.3.1 Sicherheits-analyse		X	✓	X	(✓)	X	✓	X
2.3.2 Funktion der Website	(✓)		(✓)	X	(✓)	X	(✓)	X
2.3.3 Nutzungsmessung	(✓)	(✓)	X	✓	(✓)	(✓)	(✓)	(✓)

2.3.4 Individualisierung		(✓)	(✓)					(✓)
2.3.5 Nutzerkonten				(✓)				X
2.3.6 Kontakt	X	X	X	✓	✓	X	(✓)	X
2.3.7 Newsletter	X	(✓)	✓	✓	✓	(✓)	X	✓
2.3.8 Plugins	(✓)	(✓)	X				X	X
2.3.9 Drittplattformen	✓	X		(✓)	✓	(✓)		
2.3.10 Kommentare						X		
2.3.11 Bewerbungsverfahren	✓		X				(✓)	X
2.3.12 Sonstige	X		✓	X		✓	✓	
	X					(✓)	✓	
2.4 Daten	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2.5 Zwecke	X	X	X	X	(✓)	X	X	(✓)
2.6 Rechtsgrundlage	X	X	X	X	✓	X	✓	X
2.7 Berechtigtes Interesse	(✓)	(✓)	(✓)	✓	X	(✓)	(✓)	X
2.8 Empfänger	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)

2.9 Übermittlung in Drittland	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2.10 Speicher-dauer	(✓)	(✓)	✓	X	X	✓	(✓)	(✓)
2.11 Betroffenen-rechte	X	(✓)	(✓)	X	(✓)	X	(✓)	(✓)
2.12 ggf. Wider-rufsmögl.	(✓)	(✓)	✓	✓	✓	(✓)	(✓)	✓
2.13 Beschwerde-recht	(✓)	✓	✓	✓	✓	✓	✓	(✓)
3. Bearbeitungsstand, Information über Änderungen								
	✓	✓	✓	(✓)	✓	✓	✓	✓
Grundlage der Untersuchung ist die Version vom:	18.08.2021	30.08.2021	30.08.2021	30.08.2021	30.08.2021	01.12.2021	31.08.2021	30.08.2021

✓	Vorgaben vollständig umgesetzt
(✓)	Verbesserungsmöglichkeiten
(✓)	Verbesserungsbedarf
X	Rechtliche Vorgaben nicht umgesetzt
	Prüfungs- oder Ergänzungsbedarf
	Keine Datenverarbeitung / Angabe

	BR Media-thek	Dlf Audio-thek	3Sat Medi-athek	SR Media-thek	UnserDing (SR)	WDR AR 1933-1945	DieMaus (WDR)	ZDF Medi-athek
1. Transparente Information								
1.1 leicht zugäng-lich	(✓)	(✓)	(✓)	(✓)	(✓)	✓	(✓)	✓
1.2 präzise	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
1.3 transpa-rent	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
1.4 verständ-lich	(✓)	(✓)	(✓)	(✓)	(✓)	✓	✓	(✓)
1.5 schriftlich	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
1.6 bes. Schutz-gruppen	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2. Vollständige und richtige Angaben								
2.1 Verant-wort-licher	(✓)	X	(✓)	✓	X	(✓)	(✓)	(✓)
2.2 ggf. DSB	✓	(✓)	✓	✓	X	✓	✓	✓
2.3 Datenverarbeitungsvorgänge								
2.3.1 Sicher-heits-analyse	X	(✓)	X			X	X	
2.3.2 Funktion der App			X	(✓)	(✓)	X	X	
2.3.3 Nutzungs-messung	(✓)	(✓)	(✓)	(✓)		(✓)	(✓)	(✓)

2.3.4 Individualisierung	X		X					X
2.3.5 Nutzerkonten	X							(✓)
2.3.6 Kontakt		X		X	X	X	X	X
2.3.7 Newsletter								
2.3.8 Plugins	(✓)	(✓)		(✓)				(✓)
2.3.9 Drittplattformen				(✓)		X	X	
2.3.10 Kommentare								
2.3.11 Bewerbungsverfahren								
2.3.12 Sonstige					X			
Zusätzliche Anforderungen an Apps								
2.3.13 Herunterladen				✓	✓	✓	✓	
2.3.14 Push-Benachrichtigungen				✓		(✓)	(✓)	
2.3.15 Berechtigungen				(✓)				
2.3.16 Offline-Betrieb								
2.4 Daten	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2.5 Zwecke	(✓)	(✓)	(✓)	(✓)	X	(✓)	(✓)	(✓)

2.6 Rechtsgrund-lage	X	X	X	X	X	X	X	X
2.7 Berechtigtes Interesse	(✓)	(✓)	X	(✓)	(✓)	(✓)	(✓)	X
2.8 Empfänger	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
2.9 Übermittlung in Drittland	(✓)	(✓)	(✓)	(✓)	(✓)	✓	✓	(✓)
2.10 Speicher-dauer	✓	X	(✓)	(✓)	X	(✓)	(✓)	(✓)
2.11 Betroffenen-rechte	(✓)	X	(✓)	(✓)	X	X	X	(✓)
2.12 ggf. Wider-rufsmögl.	(✓)	(✓)	(✓)	✓	(✓)	(✓)	(✓)	(✓)
2.13 Beschwerde-recht	(✓)	X	(✓)	✓	X	✓	✓	✓
3. Bearbeitungsstand, Information über Änderungen								
	✓	(✓)	(✓)	(✓)	(✓)	✓	✓	(✓)
Grundlage der Untersuchung ist die Version vom:	10.12.2021	10.12.2021	10.12.2021	10.12.2021	10.12.2021	10.12.2021	10.12.2021	07.12.2021

✓	Vorgaben vollständig umgesetzt
(✓)	Verbesserungsmöglichkeiten
(✓)	Verbesserungsbedarf
X	Rechtliche Vorgaben nicht umgesetzt
	Prüfungs- oder Ergänzungsbedarf
	Keine Datenverarbeitung / Angabe