Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten für das Jahr 2020

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

Im Tätigkeitsbericht für das Jahr 2019 bin ich ausführlich auf die wichtigsten Grundlagen und Rahmenbedingungen für den Datenschutz und die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk eingegangen. In diesem Zusammenhang habe ich die Gewährleistung von Datenschutz und Informationssicherheit als „systemrelevant" für den öffentlich-rechtlichen Rundfunk bezeichnet. Nur wenige Tage nach der Veröffentlichung des Berichts war dieser bis dahin wenig gebräuchliche Begriff unversehens in aller Munde, als die Corona-Pandemie in Deutschland zum ersten „Lockdown" führte. Unabhängig davon, ob man den Stellenwert des Datenschutzes für den öffentlich-rechtlichen Rundfunk mit ihm zutreffend beschrieben sieht oder nicht: in jedem Falle hat er virenfest zu sein. Und zwar im doppelten Sinn des Wortes: Die mit der DSGVO erst vor kurzem auf eine neue Basis und ein neues Niveau gestellten europäischen datenschutzrechtlichen Gewährleistungen dürfen auch in einer solchen Sondersituation nicht einfach zur Disposition gestellt werden. Und der Schutz gegen elektronische Viren und andere Gefahren für die Sicherheit der Datenverarbeitung erhält angesichts der rasanten Digitalisierung und Dezentralisierung der Arbeitswelt noch einmal einen deutlich höheren Stellenwert.

Von den Themen, die mich im vergangenen Jahr inhaltlich und zeitlich besonders beschäftigt haben, seien hier nur die Datenschutzprüfungen, zum anderen etliche Verfahren rund um programmliche Großvorhaben genannt, die auf teils heftige Kritik stießen. Die große Bandbreite an inhaltlichen Anliegen, die an mich herangetragen wurden, belegt das Interesse der Bevölkerung an und die Sensibilität für einen wirksamen Datenschutz im öffentlich-rechtlichen Rundfunk. Gravierende Datenschutzverstöße habe ich erfreulicherweise weder bei den Rundfunkanstalten noch bei ihren Beteiligungsunternehmen feststellen müssen. Allerdings sind meine Möglichkeiten zur intensiveren Kontrolle aus Kapazitätsgründen generell – nicht nur wegen der aktuellen Beschränkungen - begrenzt.

Selbstverständlich hat sich die Pandemie auch auf den beruflichen Alltag meiner Aufsichtsbehörde ausgewirkt. Wenigstens aber war deren Funktions- und Handlungsfähigkeit zu keinem Zeitpunkt ernsthaft beeinträchtigt. Glück im Unglück: Gerade noch rechtzeitig vor dem Eintritt dieses unvorhersehbaren Ereignisses war es uns gelungen, endlich auf ein elektronisches Aktenverwaltungssystem umzustellen. Nur deshalb – und dank der tatkräftigen Unterstützung durch den IT-Support unseres Auftragsverarbeiters, des Rundfunk Berlin-Brandenburg - waren wir in der Lage, für den Rest des Jahres relativ zügig einen weitgehenden „Fernbetrieb" vom heimischen Arbeitsplatz aus zu organisieren. Und von einer Corona-Erkrankung blieben wir ebenfalls verschont.

Den Datenschutzbeauftragten in meinem Zuständigkeitsbereich danke ich für die erneut konstruktive Zusammenarbeit und den offenen Austausch. Außerdem gilt mein herzlicher Dank meinen beiden Kolleginnen, die mit mir das kleine Team der gemeinsamen Datenschutzaufsicht für BR, SR, WDR, Deutschlandradio und ZDF sowie ihre Gemeinschaftseinrichtungen und Beteiligungsgesellschaften bilden. Gemeinsam ist es uns gelungen, das zumindest in organisatorischer Hinsicht unruhige Fahrwasser des vergangenen Jahres ohne größere logistische Probleme zu durchqueren.

Potsdam, Februar 2021
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 Nach Art. 59 DSGVO erstellt jede Aufsichtsbehörde einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen nach Art. 58 Abs. 2 DSGVO enthalten kann. Dieser Bericht wird dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden übermittelt. Er ist der Öffentlichkeit, der Kommission und dem Europäischen Datenschutzausschuss (Art. 68 DSGVO) zugänglich zu machen.

2 Die für mich maßgeblichen Landesrundfunkgesetze bzw. Staatsverträge sehen unter Bezugnahme auf Art. 59 DSGVO im wesentlichen gleichlautend vor, dass der Rundfunkdatenschutzbeauftragte den Bericht jährlich „auch den Organen" der Rundfunkanstalt bzw. Körperschaft erstattet[1]. Ebenfalls gleichlautend schreiben alle Vorschriften (entsprechend der Vorgabe von Art. 59 DSGVO) eine Veröffentlichung des Berichts vor, wobei sie eine solche im Onlineangebot der jeweiligen Rundfunkanstalt bzw. Körperschaft für ausreichend erklären. Eine – letztlich deklaratorische - Vorgabe zur Veröffentlichung in inhaltlicher Hinsicht enthält lediglich Art. 21 Abs. 9 S. 2 BR-Gesetz; danach hat der Bericht die Betriebs- und Geschäftsgeheimnisse des Bayerischen Rundfunks sowie die personenbezogenen Daten seiner Beschäftigten zu wahren.

3 Nach meinem Verständnis dieser Vorschriften und mit Blick auf das auch für die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk maßgebliche Gebot der Staatsferne erstatte ich diesen Tätigkeitsbericht in erster Linie den (jeweils drei) Organen der fünf Rundfunkanstalten in meinem Zuständigkeitsbereich. Die meisten Kollegialorgane der Anstalten haben mich dazu in eine Präsenz- oder „Digital"-Sitzung eingeladen, in der ich den Bericht kurz erläutert und Fragen beantwortet habe. Die jeweiligen Landesregierungen und -parlamente, darunter die der beiden im Jahr 2020 für das ZDF (Brandenburg) und das Deutschlandradio (Sachsen) rechtsaufsichtsführenden Länder, habe ich schriftlich darüber informiert, dass der Tätigkeitsbericht erschienen ist und auf meiner Homepage[2] zum Download zur Verfügung steht; dort ist auch der aktuelle Bericht abrufbar. Der Ausschuss für Wissenschaft, Hochschule, Medien, Kultur und Tourismus des Sächsischen Landtags hat mich daraufhin zu einer Sitzung Ende Juni 2020 eingeladen und sich einige Themen des Berichts eingehend erläutern lassen. Die Rundfunkanstalten in meinem Zuständigkeitsbereich haben den Tätigkeitsbericht (im folgenden: TB 2019), wie nach dem für sie jeweils maßgeblichen Landesrecht ausdrücklich vorgesehen, entweder unmittelbar in ihrem Onlineangebot zur Verfügung gestellt oder aber ihren Nutzern durch Verlinkung auf meine Homepage zugänglich gemacht.

---

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

2 https://www.rundfunkdatenschutz.de/infothek/taetigkeitsbericht-20190.file.html/TB%202019.pdf

1 Datenschutz und Datenschutzaufsicht: Grundlagen

a Gesetzgebung

aa) Europa

4 Seit dem 25. Mai 2018 gilt die DSGVO in allen EU-Mitgliedstaaten unmittelbar, darüber hinaus auch in Norwegen, Island und Liechtenstein, die dem Abkommen über den Europäischen Wirtschaftsraum (EWR) beigetreten sind. Zu den Auswirkungen der DSGVO auf das System der Datenschutzaufsicht habe ich mich bereits eingehend geäußert (TB 2019, Rn. 17 – 22). Gemäß deren Art. 97 Abs. 1 hatte die EU-Kommission dem Europäischen Parlament zum 25. Mai 2020 einen ersten Bericht über die Bewertung und Überprüfung der DSGVO vorzulegen. Diesen Bericht zur **Evaluation der DSGVO** hat die Kommission gem. Art. 97 Abs. 1 S. 2 DSGVO auch veröffentlicht[3]. Diese soll sich nach Abs. 2 insbesondere auf die Anwendung und Wirkungsweise des Kapitels V zur Datenübermittlung an Drittländer sowie des Kapitels VII zur Zusammenarbeit und Kohärenz der Aufsichtspraxis auf europäischer Ebene beziehen. Dazu kann die Kommission unter anderem Informationen von den Mitgliedstaaten und den Aufsichtsbehörden anfordern, Art. 97 Abs. 3 DSGVO.

5 Der Evaluationsbericht hebt die weltweite Vorreiterrolle der DSGVO für einen wirksamen Schutz des Grundrechts auf Datenschutz hervor, etwa mit Blick auf die Covid 19-Pandemie oder den Schutz demokratischer Prozesse, insbesondere im Zusammenhang mit Wahlen (S. 3 f.). Zwei der zentralen Ziele der DSGVO – die Stärkung des Rechts des Einzelnen auf Schutz personenbezogener Daten sowie die Gewährleistung des freien Verkehrs personenbezogener Daten innerhalb der EU – sieht die Kommission als erreicht an. Sie benennt jedoch auch einige Bereiche, in denen noch weitere Erfahrungen zu sammeln seien, um das Regelwerk gegebenenfalls punktuell zu optimieren.

6 Die Kommission stellt fest, dass die Datenschutzbehörden ihre Zusammenarbeit zwar ausgebaut haben. Eine wirklich gemeinsame europäische Datenschutzkultur zwischen ihnen müsse sich jedoch noch entwickeln (S. 6, 17 f.). Bisweilen ende die Suche nach einem gemeinsamen Ansatz noch – wie etwa bei der Entwicklung der nationalen Listen der Arten von Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich ist - mit einer Einigung auf den kleinsten gemeinsamen Nenner (S. 6). Auch die Ausstattung der Datenschutzbehörden sei von Mitgliedstaat zu Mitgliedstaat noch sehr uneinheitlich und insgesamt nicht zufriedenstellend. Insoweit wird zurecht vielfach kritisiert, dass die steuerlich motivierte Standortentscheidung insbesondere US-amerikanischer Internetkonzerne mit ihren marktbeherrschenden Plattformen dazu führt, dass kleine Datenschutzbehörden – wie etwa im Falle von Facebook die irische – mit ihren beschränkten Ressourcen federführend die wichtigsten und komplexesten Datenschutzverfahren für die gesamte EU führen müssen. Infolge dieses „Flaschenhalses" verzögern sich verbindliche Entscheidungen zum Verständnis und zur Anwendung grundlegender

[3] Mitteilung der Kommission an das Europäische Parlament und den Rat: Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung vom 24. Juni 2020; COM (2020) 264 final, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0264&from=EN

Vorschriften der DSGVO unnötig lang. Die Kommission ist auf die damit verbundenen Verfahrensfragen in ihrem ersten Evaluationsbericht allerdings nicht näher eingegangen, sondern hat sich auf die Forderung an die Mitgliedstaaten beschränkt, den Datenschutzbehörden angemessene Ressourcen zur Verfügung zu stellen (S. 7).

7 Besonderes Augenmerk widmet die Kommission auch dem Verhältnis des Rechts auf Schutz der personenbezogenen Daten zur Meinungs- und Informationsfreiheit. Deren Vereinbarkeit müsse den Anforderungen von Art. 52 Abs. 1 der Europäischen Grundrechtecharta (GRCh) entsprechen, und die Auslegung und Anwendung der Datenschutzvorschriften dürfe die Ausübung der Meinungs- und Informationsfreiheit nicht einschränken, indem beispielsweise eine abschreckende Wirkung geschaffen oder Druck auf Journalisten zur Preisgabe ihrer Quellen ausgeübt wird (S. 8 f.). Diesen Vorgaben trägt das deutsche Datenschutzrecht nicht nur durch die Vorschriften zum sogenannten „Medienprivileg" (dazu ausführlich TB 2019, Rn. 4 ff.), sondern gerade auch durch die Ausgestaltung einer rundfunk- bzw. medienspezifischen Aufsichtsstruktur Rechnung. So verbindet die Aufsicht durch einen Rundfunkdatenschutzbeauftragten die durch Art. 51 DSGVO geforderte vollständige Unabhängigkeit (sowohl gegenüber den Rundfunkanstalten als auch gegenüber den staatlichen Institutionen) mit einer fachlichen Nähe zu allen Fragen der Informations-, Meinungs- sowie Rundfunkfreiheit, die bei den allgemeinen Datenschutzaufsichtsbehörden nicht ohne weiteres vorhanden ist bzw. hergestellt werden kann.

8 Ein dritter und letzter Punkt des Evaluationsberichts sei hier noch erwähnt: Die Kommission geht auch auf den in Politik und Öffentlichkeit vielfach erhobenen Vorwurf ein, dass die Anforderungen der DSGVO kleine und mittlere Unternehmen (KMU) unverhältnismäßig belasteten. Sie weist darauf hin, dass es der risikobasierte Ansatz der DSGVO verbiete, allein auf die Größe eines Unternehmens abzustellen. In der Tat können natürlich auch KMU in erheblichem Umfang personenbezogene Daten verarbeiten. Wohl aber will die Kommission punktuell Möglichkeiten erkunden, um KMU dort, wo sich dies als sinnvoll oder erforderlich erweist, zu unterstützen oder zu entlasten (S. 12 f.). Dazu zählt auch die Prüfung, ob die Vorschriften zum Verzeichnis von Verarbeitungstätigkeiten für KMU, deren Kerngeschäft nicht die Verarbeitung personenbezogener Daten ist, modifiziert werden können (S. 19) – ein Anliegen, das die meist kleinen Beteiligungsgesellschaften der Rundfunkanstalten in meinem Zuständigkeitsbereich nachdrücklich unterstützen dürften.

9 Parallel zur DSGVO wollte die EU-Kommission auch die bisherige E-Privacy-Richtlinie (2002/58/EG[4]) durch eine EU-Verordnung ablösen, die – im Gegensatz zu einer Richtlinie – in den Mitgliedstaaten unmittelbar gilt. Dieses Vorhaben hat sie allerdings trotz mehrerer Anläufe bisher nicht abschließen können: ihr bereits vom 10. Januar 2017 datierender Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 010 final – 2017/03 (COD)[5] –, die sogenannte **ePrivacy-Verordnung**, konnte auch während der deutschen Ratspräsidentschaft 2020 nicht umgesetzt werden, weil sich die Mitgliedstaaten noch nicht auf einen Kompromiss zu

4 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32002L0058&qid=1580735840113
5 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52017PC0010&from=EN

einigen zentralen Vorschriften einigen konnten. Bis auf weiteres gelten daher die Vorschriften der E-Privacy-Richtlinie, und sie verdrängen die Regelungen der DSGVO, soweit sie a) vergleichbare Regelungsziele verfolgen und b) in nationales Recht umgesetzt worden sind. Nach ihrem Art. 3 richtet sich die E-Privacy-Richtlinie in erster Linie an Anbieter von Telekommunikationsdiensten (im Sinne des Telekommunikationsgesetzes) sowie teilweise an Anbieter von Telemedien (im Sinne des Telemediengesetzes). Für die Rundfunkanstalten und ihre Beteiligungsgesellschaften ist dies vor allem insoweit relevant, als es um den Einsatz sogenannter Cookies zur Erfassung von Nutzungsdaten in ihren Onlineangeboten geht. Hierzu enthält § 15 TMG spezifische Vorschriften. Ob sie allerdings mit den Vorgaben der Richtlinie vereinbar sind und damit deren Vorgaben wirksam in nationales Recht umgesetzt haben, ist seit Jahren umstritten (s. dazu auch unten Rn. 33 f.).

10 Zwei weitere große Gesetzgebungsvorhaben mit vor allem wettbewerbs-, zumindest mittelbar aber auch datenschutzrechtlichem Bezug hat die EU-Kommission Ende 2020 offiziell eingeleitet: Der Entwurf eines Digitale-Dienste-Gesetzes (**Digital Services Act**[6]) sowie eines Digitale-Märkte-Gesetzes (Digital Market Act) soll neue Rahmenbedingungen für die jeweils marktbeherrschenden US-amerikanischen Internetkonzerne wie Google, Facebook, Amazon oder Apple schaffen und bestimmte Geschäftspraktiken verhindern bzw. verbieten. Dazu zählt nicht zuletzt der mit den Vorgaben der DSGVO häufig nicht oder allenfalls eingeschränkt vereinbare Umgang mit den personenbezogenen Daten der Nutzer der von diesen Unternehmen angebotenen Dienste. So sollen es die neuen Regeln unter anderem ermöglichen, die „Datenmacht" der Internetkonzerne als Marktvorteil zu qualifizieren und diese insoweit der Aufsicht einer neuen europäischen Behörde zu unterstellen – durchaus auch mit Blick auf die Erfahrung, 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 (s. oben Rn. 6). Die neue Kommissionspräsidentin hat das Gesetzespaket zu einem der Leuchtturmprojekte ihrer Amtsperiode erklärt. Es bleibt abzuwarten, ob es in dieser Zeit tatsächlich in Kraft treten kann.

11 Handlungs- bzw. Regelungsbedarf löste schließlich auch der zum 31. Januar 2020 vollzogene **Brexit** aus. Das dazu nach langwierigen Verhandlungen erst kurz vor dem Jahresende zustande gekommene Abkommen zwischen der EU und dem Vereinigten Königreich Großbritannien und Nordirland sieht eine viermonatige Übergangsfrist für Datentransfers nach Großbritannien ab dem 1. Januar 2021 vor, die auf sechs Monate verlängert werden kann. Anderenfalls hätten mit Beginn des Jahres 2021 personenbezogene Daten in das Vereinigte Königreich nur noch unter den Voraussetzungen der Artt. 45 ff. DSGVO übermittelt werden können. In der Übergangszeit soll die EU-Kommission tragfähige Entscheidungen über die Angemessenheit des Datenschutzniveaus im Vereinigten Königreich vorlegen, die die aktuelle Rechtsprechung des Europäischen Gerichtshofs (EuGH) – insbesondere im Verfahren „Schrems II" (s. dazu unten Rn. 26 f.) - berücksichtigen.

---

[6] Regulation of the European Parliament and of the Council on a Single Market For digital Services and amending Directive 200/31/EC vom 15.12.2020, COM (2020) 825 final; https://eur-lex.europa.eu/legal-content/de/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN

bb) Deutschland

12 Das seit 1. Oktober 2017 geltende Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz, NetzDG) soll es Nutzerinnen und Nutzer von sogenannten sozialen Netzwerken ermöglichen bzw. erleichtern, sich gegen dort – oft anonym oder pseudonym - veröffentlichte Drohungen oder Beleidigungen zur Wehr zu setzen. Am 1. April 2020 hat die Bundesregierung ein Änderungsgesetz zum NetzDG beschlossen, das das dafür eingeführte Instrumentarium ergänzen bzw. optimieren soll[7]. So kann die betroffene Person bislang vom Betreiber des sozialen Netzwerks Informationen – wie etwa den Namen des Urhebers -, die sie zur Durchsetzung ihrer Rechte benötigt, erst verlangen, nachdem das angerufene Gericht die Zulässigkeit dieses Anspruchs festgestellt hat. In der Praxis führt dies immer wieder dazu, dass der Netzwerkbetreiber die Herausgabe der Daten mit dem Argument verweigert, er sei dazu gleichwohl nicht verpflichtet. Daher soll unter anderem § 14 Telemediengesetz (TMG) dahingehend ergänzt werden, dass Betroffene künftig den Plattformbetreiber gerichtlich auch zur Herausgabe der Daten des – anonymen oder pseudonymen – Urhebers verpflichten können. Der Gesetzesentwurf wird derzeit noch im Bundestag beraten.

13 Weiterverfolgt hat die Bundesregierung auch ihr Vorhaben, das BSI-Gesetz zu novellieren (dazu bereits TB 2019, Rn. 35 – 37). Der am 16. Dezember 2020 beschlossene Kabinettsentwurf für ein Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)[8] 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 womöglich auch den öffentlich-rechtlichen Rundfunk in Deutschland betroffen (dazu ausführlich TB 2019, Rn. 36 f.). Eine dahingehende Vorschrift enthält der nun verabschiedete Kabinettsentwurf nicht mehr. Ebenfalls ist entgegen der ursprünglichen Fassung keine Speicherpflicht für Systeme zur Angriffserkennung (dazu TB 2019, Rn. 160 ff.) mehr vorgesehen.

14 Im Sommer 2020 wurde der Entwurf eines vom Bundesministerium für Wirtschaft und Energie (BMWi) geplanten Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG-E) bekannt[9]. Es soll die Rechtsunsicherheit beseitigen, die durch das ungeklärte Verhältnis zwischen den Vorschriften der DSGVO und ePrivacy-Richtlinie einerseits sowie des TMG und TKG andererseits in Bezug auf den Datenschutz und den Schutz der Privatsphäre in

---

7 https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Aenderung_NetzDG.pdf?__blob=publicationFile&v=2

8 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicher-heitsgesetz.pdf;jsessionid=30ED742168F149BC893E1B10894D4C3E.2_cid373?__blob=publicationFile&v=2

9 https://cdn.netzpolitik.org/wp-upload/2020/08/20200731_RefE_TTDSG-clean.pdf

der Telekommunikation und bei Telemedien entstanden ist (oben Rn. 9), nicht zuletzt mit Blick auf die jüngste Rechtsprechung des Bundesgerichtshofs zur Auslegung von § 15 Abs. 3 TMG (dazu unten Rn. 33 f.). Die Begründung des Gesetzesentwurfs sieht Klarstellungsbedarf vor allem im Hinblick auf das Einwilligungserfordernis der sog. Cookie-Regelung in Art. 5 Abs. 3 ePrivacy-Richtlinie. Insofern kann die Neuregelung (§ 9 des Entwurfs) auch Konsequenzen für die von den Rundfunkanstalten durchgeführte Nutzungsmessung ihrer Telemedienangebote haben (s. dazu TB 2019, Rn. 181 ff.). Daneben bezeichnet § 27 Abs. 1 S. 2 des Entwurfs den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit pauschal als „zuständige Aufsichtsbehörde" über die Einhaltung der im Gesetzesentwurf vorgesehenen datenschutzrechtlichen Bestimmungen. Dies allerdings dürfte mit der landesrechtlich festgelegten Zuständigkeit der rundfunkspezifischen Datenschutzaufsicht über die Rundfunkanstalten jedenfalls in dieser Allgemeinheit nicht vereinbar sein. Bis zum Jahresende lag jedoch entgegen dem ursprünglichen Zeitplan – der ein Inkrafttreten noch im Jahr 2020 vorgesehen hatte - noch nicht einmal ein finalisierter Referentenentwurf vor. Perspektivisch wird ein solches Gesetz dann ganz oder teilweise durch die vorgesehene EU-ePrivacy-Verordnung abgelöst werden.

15 Ebenfalls noch nicht abgeschlossen ist das schon im März 2019 begonnene Verfahren zur Verabschiedung eines „**Gesetzes zur Harmonisierung des Verfassungsschutzrechts**" (dazu TB 2019, Rn. 38). Dieses soll den Inlands- und Auslandsgeheimdiensten einen weitgehenden Zugriff auf „informationstechnische Systeme" etwa von sogenannten Gefährdern, aber auch Anbietern von Internet-Diensten, derer sich Gefährder bedienen, ermöglichen. Mithilfe eines sogenannten „Staatstrojaners" sollte ursprünglich das Bundesamt für Verfassungsschutz Server, Computer, Smartphones und sonstige Geräte unterschiedlichster Personen und Organisationen verdeckt durchsuchen können. Grundsätzlich hätte dies auch Rundfunkanstalten oder Verlage sowie deren Journalisten treffen können. Diese mit Blick auf das streng und umfassend geschützte Redaktionsgeheimnis hochproblematische Regelung ist im Lauf der Ressortabstimmung zwischen Bundesinnen- und -justizministerium zwar entfallen. Gestattet bleiben soll aber neben dem Abhören von Telefonaten und dem Zugriff auf SMS auch das Mitlesen verschlüsselter Chats; dies würde ebenfalls den Einsatz eines „Staatstrojaners" voraussetzen. Die verfassungsrechtlichen Bedenken in Bezug auf das vom „Medienprivileg" geschützte Redaktionsgeheimnis dürften damit jedenfalls nicht vollständig ausgeräumt sein.

16 Schließlich sei noch erwähnt, dass die Regierungsfraktionen mithilfe eines „Reparaturgesetzes" die Vorschriften zur sogenannten Bestandsdatenauskunft an die Vorgaben des Bundesverfassungsgerichts (s. unten Rn. 30 f.) anpassen wollen. Den entsprechenden „Entwurf eines Gesetzes zur Anpassung der **Regelungen über die Bestandsdatenauskunft** an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020" haben sie am 15. Dezember 2020 in den Bundestag eingebracht[10]. Zahlreiche Behörden sollen danach berechtigt sein, nach Maßgabe gesetzlich festgelegter Gründe in bestimmten Fällen Daten nicht nur bei Telekommunikations-, sondern auch bei unterschiedlichsten Telemedienanbietern, insbesondere aus sozialen Medien, Chats, Suchmaschinen, Communities etc. abzurufen. Ob das Gesetzesvorhaben die Rechtsprechung des BVerfG, das die aus dem Jahr 2013 stammenden Vorgängerregelungen für verfassungswidrig erklärt hatte,

[10] https://dserver.bundestag.de/btd/19/252/1925294.pdf

tatsächlich adäquat umsetzt, bleibt allerdings abzuwarten. Zumindest potentiell können die mit den entsprechenden Regelungen begründeten Eingriffsbefugnisse auch die journalistische Tätigkeit berühren.

cc) Bundesländer

17 Zuständig für die Regulierung von Rundfunk und rundfunkähnlichen Telemedien sowie die Presse sind in Deutschland grundsätzlich die Bundesländer. Das gilt auch, soweit es um die Datenschutzaufsicht über die Anbieter solcher Medien geht. Dementsprechend haben die Bundesländer im neuen **Medienstaatsvertrag** (MStV), der seit dem 7. November 2020 den vormaligen Rundfunkstaatsvertrag ersetzt, ausdrücklich festgehalten, dass „für die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio und private Rundfunkveranstalter sowie zu diesen gehörende Beteiligungs- und Hilfsunternehmen … die Aufsicht über die Einhaltung der geltenden datenschutzrechtlichen Bestimmungen durch Landesrecht bestimmt“ wird, § 12 Abs. 4 S. 1.

18 Die für die Rundfunkanstalten maßgeblichen medienspezifischen Datenschutzvorschriften finden sich nun in den §§ 12 und 23 MStV. Insgesamt entsprechen beide Vorschriften den §§ 9c und 57 des vormaligen Rundfunkstaatsvertrags.

19 Es hätte nahegelegen, mit dem MStV, der insgesamt die Rundfunkregulierung in weiten Teilen neu ausgerichtet hat, auch die recht heterogene Datenschutzaufsichtsstruktur zumindest für den öffentlich-rechtlichen Rundfunk länderübergreifend als rundfunkspezifische Datenschutzaufsicht zu vereinheitlichen oder sogar (im Sinne einer echten Strukturreform, zu der die Länder ansonsten vorzugsweise die Rundfunkanstalten selbst auffordern) zusammenzuführen. Das ist bedauerlicherweise unterblieben. Daher sind mit dem Hessischen Rundfunk, Radio Bremen und Rundfunk Berlin-Brandenburg nach wie vor drei der neun in der ARD zusammengeschlossenen Landesrundfunkanstalten von dem von ihren Bundesländern eingeschlagenen Sonderweg betroffen, der nur die journalistische Datenverarbeitung der Rundfunkanstalt von der Aufsicht durch die jeweilige Landesdatenschutzbehörde ausnimmt und einem internen Datenschutzbeauftragten vorbehält. Noch unterschiedlicher fallen die Aufsichtsregelungen für den privaten Rundfunk sowie die Telemedienanbieter aus. Die Einzelheiten ergeben sich aus dem jeweiligen Landesmedien-, Landesrundfunk- oder Landesdatenschutzgesetz (dazu bereits TB 2019, Rn. 39, 102 f.).

b Datenschutzrelevante Entwicklungen

aa) Internationaler Datenverkehr

20 Die Rundfunkanstalten oder ihre Beteiligungsunternehmen übertragen personenbezogene Daten auch in Staaten, für die nicht die DSGVO gilt. Eine solche Datenübermittlung ist beispielsweise mit dem Einsatz von Produkten US-amerikanischer Konzerne wie Microsoft, IBM, Amazon (das mit AWS das weltweit führende Cloud-System anbietet) oder Google verbunden. Nach Art. 44 S. 1 DSGVO ist in diesen Fällen eine Datenübermittlung allerdings grundsätzlich nur zulässig, wenn die Verantwortlichen in einem solchen sogenannten Dritt-

land 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 auch 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.

21 Indessen wären die Verantwortlichen mit einer Prüfung, ob Drittstaaten ein der DSGVO vergleichbares 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 entsprechende Prüfung durch die EU-Kommission vor, deren Ergebnis ein sogenannter Angemessenheitsbeschluss sein kann. Eine darauf gestützte Datenübermittlung an ein Drittland bedarf gem. Art. 45 Abs. 1 S. 2 DSGVO keiner besonderen Genehmigung.

22 Falls ein solcher Beschluss nicht vorliegt, macht Art. 46 DSGVO die Übermittlung personenbezogener Daten an ein Drittland davon abhängig, dass die Standards der DSGVO durch anderweitige geeignete Garantien abgesichert sind und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Dazu können unter anderem von der Kommission genehmigte Standarddatenschutzklauseln gehören, Art. 46 Abs. 2 DSGVO. Das außerdem erforderliche Einverständnis der Vertragspartner ist den US-amerikanischen Großkonzernen freilich erfahrungsgemäß nur unter größtem Aufwand und mit entsprechendem Nachdruck, insbesondere also Verhandlungen auf hoher Ebene, abzuringen. Ausnahmen von diesen Vorgaben sieht Art. 49 DSGVO nur für bestimmte Fälle und unter engen Voraussetzungen vor.

23 Bislang hat die Kommission etwa ein Dutzend Angemessenheitsentscheidungen veröffentlicht[11]. Mit Abstand die größte Bedeutung hat insoweit das Verhältnis zu den **USA**. Den ursprünglichen Beschluss der Kommission, die Datenübermittlung auf der Grundlage des sogenannten „Safe-Harbor"-Abkommens mit dem US-Handelsministerium für angemessen zu erklären, hatte der EuGH bereits im Oktober 2015 für ungültig erklärt[12]. Das gleiche Schicksal ereilte das anschließend stattdessen geschlossene Abkommen zum US-Privacy-Shield bzw. den darauf bezogene Angemessenheitsbeschluss der Kommission: Mit seinem Urteil vom 16. Juli 2020 – C 311/18 - machte der EuGH erneut unmissverständlich klar, dass er nicht bereit ist, Abstriche vom Schutzniveau der DSGVO hinzunehmen (siehe unten Rn. 26 f.). Die Zweifel an der Vergleichbarkeit des Datenschutzniveaus in den USA mit den Standards der DSGVO beziehen sich auch auf den im März 2018 in Kraft getretenen sogenannten CLOUD (Clarifying Lawful Overseas Using of Data)-Act, der US-amerikanische Unternehmen verpflichtet, den dortigen Behörden einen Datenzugriff zu ermöglichen, unabhängig davon, wo die Speicherung stattfindet. Weitergehende datenschutzrechtliche Anforderungen als in den USA sonst üblich enthält bislang lediglich der zum 1. Januar 2020 in Kraft getretene California Consumer Privacy Act (CCPA), der zwar primär das Ziel des Verbraucherschutzes verfolgt, aber zahlreiche Garantien der DSGVO übernommen hat.

---

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

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

24 Vor diesem Hintergrund ist die Inanspruchnahme von Dienstleistungen der großen US-amerikanischen Konzerne, insbesondere soweit es um Büroanwendungen, die Nutzung von Videokonferenz- und sonstigen Systemen für die Zusammenarbeit auf elektronischem Weg sowie um IT-Infrastrukturen wie etwa die Cloud-Speicherung geht, unverändert mit erheblichen Risiken in Bezug auf die Gewährleistungen von Datenschutz und Datensicherheit verbunden. Mindestens ebenso gewichtig sind die strategischen Konsequenzen einer zunehmenden Abhängigkeit von den betreffenden Anbietern (dazu bereits TB 2019, Rn. 45 mit Fn. 25). Selbstverständlich stehen vor diesem Problem nicht nur die Verantwortlichen in meinem Zuständigkeitsbereich, sondern alle Anwender in der EU. Dies enthebt allerdings keinen von ihnen von der Verpflichtung, sich mit allen damit verbundenen Gefahren insbesondere für Datenschutz und Informationssicherheit gründlich zu befassen, die für sie jeweils maßgeblichen Gesichtspunkte zu bewerten und die Gründe für ihre Entscheidung zu dokumentieren, Art. 5 Abs. 2 DSGVO.

25 Ein Angemessenheitsbeschluss fehlt auch noch im Verhältnis zum bisherigen EU-Mitglied **Großbritannien**, das die EU am 31. Januar 2020 verlassen hat. Es bleibt abzuwarten, ob die EU-Kommission innerhalb der noch bis längstens Mitte 2021 geltenden Übergangsfrist (s. oben Rn. 11) Klarheit über die künftigen Rahmenbedingungen des Datenverkehrs dorthin herbeiführen kann.

bb) Rechtsprechung auf europäischer Ebene

26 Auch im Jahr 2020 hat sich der **Europäische Gerichtshof** (EuGH) wieder mit dem europäischen und damit auch nationalen Datenschutzrecht befasst. Nicht unbedingt überraschend, aber gleichwohl aufsehenerregend war seine Entscheidung zum Datenverkehr zwischen den Mitgliedstaaten der Europäischen Union und den Vereinigten Staaten. Es ist bereits die zweite, die der österreichische Datenaktivist Schrems in einem Beschwerdeverfahren gegen die Irische Datenschutzaufsichtsbehörde erstritt. In beiden Fällen ging es um die Datenübermittlung durch Facebook. Mit Urteil vom 16. Juli 2020 – C-311/18 – (Schrems II)[13] erklärte der EuGH den sogenannten EU-US-Privacy Shield für ungültig, weil das Abkommen nicht den der DSGVO vergleichbaren angemessenen Schutz der personenbezogenen Daten von EU-Bürgern gewährleisten könne, den Art. 45 DSGVO mit Blick auf die in Art. 7, 8 und 47 GRCh verbürgten Grundrechte fordere. Dies liege insbesondere an den weitreichenden Überwachungs- und Zugriffsbefugnissen der US-amerikanischen Geheimdienste, die mit dem unionsrechtlichen Grundsatz der Verhältnismäßigkeit nicht vereinbar seien. Zudem hätten betroffenen Personen keine ausreichenden Möglichkeiten, ihr Recht auf Achtung des Privatlebens und den Schutz ihrer personenbezogenen Daten wirksam durchzusetzen. Einen effektiven Rechtsschutz könne auch die im Privacy-Shield vorgesehene Ombudsperson nicht gewährleisten, weil sie dem US-amerikanischen Außenminister unterstehe und daher nicht als hinreichend unabhängig anzusehen sei. Zudem verfüge sie

13 http://curia.europa.eu/juris/document/document.jsf?text=privacy%2Bshield&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=531727#ctx1

nicht über ausreichende Kompetenzen, um gegenüber den Geheimdiensten verbindlich entscheiden zu können.

27 Der EuGH setzt damit seine Rechtsprechung zum Stellenwert eines wirksamen Datenschutzes in der EU und dessen Durchsetzung auch über die EU hinaus bemerkenswert konsequent fort. Dazu gehört, dass er (erneut) keine Übergangsfrist vorgesehen hat, innerhalb derer die EU-Kommission womöglich neue Rahmenbedingungen für den Datentransfer in die USA hätte schaffen können. Vielmehr ist seit der Entscheidung jede auf das US Privacy Shield gestützte Datenübermittlung in Drittländer per se unzulässig.

28 Diese Rechtslage löst unmittelbaren Handlungsbedarf für jeden Verantwortlichen aus, der beispielsweise Anwendungen US-amerikanischer Hersteller einsetzt, die personenbezogene Daten Dritter in die USA übermitteln; davon sind auch die Rundfunkanstalten nicht etwa ausgenommen. Zwar hat der EuGH in seiner Entscheidung vom 16. Juli 2020 die von der EU-Kommission nach Art. 46 DSGVO beschlossenen Standarddatenschutzklauseln als grundsätzlich weiterhin wirksam angesehen. Allerdings hält er nicht die Kommission, sondern die Vertragsparteien und hier vor allem den Datenexporteur dafür verantwortlich, in jedem Einzelfall zu prüfen, ob das auf den Datenimporteur anwendbare Recht des Bestimmungslands die übermittelten Daten in vergleichbarer Weise schützt wie die DSGVO. Nötigenfalls müsse er über die Standarddatenschutzklauseln hinausgehende zusätzliche Maßnahmen ergreifen bzw. vereinbaren, um die Einhaltung des erforderlichen Schutzniveaus wirksam zu gewährleisten und durchzusetzen. Mehr noch: der Verantwortliche hat auch fortlaufend zu überprüfen, ob die vertraglich vereinbarten Maßnahmen effektiv umgesetzt werden und wirken. Anderenfalls ist eine Datenübermittlung in ein Drittland – insbes. die USA – unzulässig, und die zuständige Aufsichtsbehörde ist gehalten, sie gegebenenfalls auch zu unterbinden (Urt. Rn. 134 f.).

29 Zu den sich aus der Entscheidung ergebenden Handlungspflichten der Verantwortlichen hat die RDSK im August 2020 Empfehlungen verabschiedet[14]. Ergänzende und vertiefende Hinweise enthalten die vom Europäische Datenschutzausschuss am 10. November 2020 veröffentlichten Leitlinien[15]. Beide ermöglichen den Verantwortlichen eine erste Orientierung. Sie müssen der Datenschutzaufsicht ihre Bemühungen um eine wirksame Durchsetzung eines der DSGVO entsprechenden Datenschutzniveaus gegebenenfalls nachweisen.

cc) Deutschland

30 Auch das **Bundesverfassungsgericht** (BVerfG) hatte sich bereits zum zweiten Mal mit einund derselben spezifischen Frage zu befassen, nämlich unter welchen Voraussetzungen der staatliche Zugriff auf Telekommunikationsdaten gegen das durch Art. 2 Abs. 1 GG geschützte Recht auf informationelle Selbstbestimmung verstößt. Mit Beschluss vom 27. Mai

[14] https://www.rundfunkdatenschutz.de/infothek/empfehlung-rdsk-is-privacy-shield.file.html/Empfehlung%20RDSK%20iS%20Privacy%20Shield%2020200820.pdf
[15] https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

2020 – 1 BvR 1873/13, 1 BvR 2618/13 – (Bestandsdatenauskunft II)[16] erklärte es Vorschriften aus mehreren Gesetzen für verfassungswidrig, die die sogenannte manuelle Bestandsdatenauskunft regelten. Diese ermöglicht es Sicherheitsbehörden, von Telekommunikationsunternehmen Auskunft etwa über den Inhaber eines Telefonanschlusses oder einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse zu erlangen. Mitzuteilen sind ihnen dann personenbezogene Daten des Kunden, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen, nicht hingegen jene, die sich auf die Nutzung des betreffenden Dienstes oder den Kommunikationsinhalt beziehen. Allerdings muss nach dem Bild einer „Doppeltür" sowohl die Übermittlung der Daten durch die Telekommunikationsanbieter als auch der Abruf der Daten durch die Behörden jeweils auf einer Rechtsgrundlage beruhen. Sie hat die Verwendungszwecke hinreichend zu begrenzen und einen angemessenen Ausgleich zwischen den jeweiligen Interessen der Gefahrenabwehr und den betroffenen Rechtsgütern herzustellen. Diese Voraussetzungen sah das BVerfG als nicht erfüllt an. Außerdem vermisste das BVerfG eine gesetzliche Vorgabe, die Entscheidungsgrundlagen des Abrufs nachvollziehbar und überprüfbar zu dokumentieren.

31 Das BVerfG hat dem Bund aufgegeben, die betreffenden Vorschriften bis spätestens Ende 2021 zu überarbeiten; bis dahin bleiben sie grundsätzlich anwendbar. Daneben sind die vom BVerfG entwickelten Maßstäbe auch für aktuelle Vorhaben wie etwa das Gesetz zur Bekämpfung der Hasskriminalität bedeutsam (s. oben Rn. 12).

32 Die gleiche Übergangsfrist räumte das BVerfG dem Bund ein, um zentrale Vorschriften des im Jahr 2017 geänderten Gesetzes über den Bundesnachrichtendienst zu überarbeiten, die den BND ermächtigen, im Zusammenhang mit der strategischen Fernmeldeaufklärung personenbezogene Daten zu verarbeiten. In seinem Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –[17] betonte es 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. Die journalistische Tätigkeit rechtfertige es nicht, „Personen einem höheren Überwachungsrisiko auszusetzen als andere Grundrechtsträger und sie wegen ihrer Kontakte und Recherchen zum Objekt der Informationsabschöpfung zur Verfolgung von Sicherheitsinteressen zu machen." 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 (Urt. Rn. 194, 257).

33 Am 1. Oktober 2019 hatte der EuGH klargestellt, dass ein Diensteanbieter das Einverständnis mit der Verarbeitung von Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, jedenfalls nicht durch ein bereits angekreuztes Einwilligungs-

[16] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200527_1bvr187313.html

[17] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html

kästchen einholen kann. Vielmehr ist dafür stets ein ohne jeden Zweifel nachweisbares aktives Verhalten erforderlich (dazu TB 2019, Rn. 55 ff.). Nur dann liege die von Art. 5 Abs. 3 der Europäischen ePrivacy-Richtlinie für diese Fälle geforderte wirksame Einwilligung vor. Ob diese Voraussetzung in dem betreffenden Fall erfüllt waren, hatte sodann der **Bundesgerichtshof** (BGH), auf dessen Vorlagebeschluss das Urteil des EuGH zurückgeht, selbst zu entscheiden. Mit Urteil vom 28. Mai 2020 – I ZR 7/16 –[18] stellte er fest, dass die vom EuGH entwickelten Grundsätze auch für Cookies gelten, die es einem Diensteanbieter ermöglichen, mithilfe von Pseudonymen Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien zu erstellen. Diese Entscheidung ist deshalb bemerkenswert, weil § 15 Abs. 3 Telemediengesetz (TMG) den Einsatz von Cookies zu diesen Zwecken eigentlich generell erlaubt, es sei denn der Nutzer hat ihm ausdrücklich widersprochen. Ungeachtet dieses Wortlauts legt der BGH die Vorschrift im Sinne von Art. 5 Abs. 3 ePrivacy-Richtlinie so aus, dass auch in den dort genannten Fällen eine ausdrückliche Einwilligung nach den Vorgaben des EuGH gefordert sei. Die Alternative wäre gewesen, § 15 Abs. 3 TMG insoweit für europarechtswidrig zu erklären (s. TB 2019, Rn. 59); dies wollte der BGH erkennbar vermeiden. Mit den klassischen Auslegungskriterien des deutschen Rechts lässt sich seine Entscheidung allerdings schwerlich in Einklang bringen.

34 Grundsätzlich ist die Frage der Zulässigkeit des Einsatzes von Cookies auch für die Rundfunkanstalten sehr bedeutsam, weil sie die publizistische Wirksamkeit ihrer Onlineangebote mithilfe entsprechender Instrumente überprüfen bzw. optimieren. Sie sehen den Erkenntniswert dieser Auswertungen in Frage gestellt, wenn sie die Cookies nur mit Einwilligung der Nutzer einsetzen dürften. Allerdings sollte § 15 Abs. 3 TMG es Telemedienanbietern nach Sinn und Zweck ermöglichen, pseudonymisierte Nutzungsprofile für die dort genannten Zwecke auch ohne Einwilligung der Betroffenen anzulegen; die Vorschrift war also als Privilegierungstatbestand gedacht. Die Rundfunkanstalten hingegen stützen sich ausschließlich auf vollständig anonymisierte Auswertungen, die keine personalisierbare, sondern ausschließlich auf ihr Onlineangebot insgesamt bezogene statistische Erkenntnisse ermöglichen. Dies unterfällt nicht dem Anwendungsbereich des § 15 Abs. 3 TMG. Unbeschadet dessen hat die RDSK mit Blick auf die Entscheidung des BGH auf der Basis eines von mir vorbereiteten Entwurfs ihre im Vorjahr veröffentlichten Empfehlungen zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten[19] im September 2020 überarbeitet (unten Rn. 106 f.).

35 Außerdem hat sich – nach dem EuGH und dem BVerfG im Vorjahr (TB 2019, Rn. 53 f., 62 ff.) – nun auch der BGH in zwei Entscheidungen mit dem „Recht auf Vergessenwerden" bzw. der Reichweite des in Art. 17 DSGVO verankerten Rechts auf Löschung befasst. Im ersten Urteil vom 27. Juli 2020 – VI ZR 405/18 –[20] wies der BGH das Löschungsbegehren des Ge-

[18] https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=53771f29989c7168953aae5fdc3b56cd&nr=107623&pos=0&anz=1

[19] https://www.rundfunkdatenschutz.de/infothek/empfehlung-rdsk-cookies.file.html/Cookie%20Empfehlungen%20RDSK%20202009%20fin.pdf

[20] https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=b72c79b743fe408e177bb530208a7ca0&nr=110285&pos=0&anz=1

schäftsführers eines Regionalverbands einer Wohlfahrtsorganisation ab, der verhindern wollte, dass Artikel der Regionalpresse, in denen er namentlich genannt worden war, weiterhin online auffindbar blieben. Wie der EuGH und das BVerfG legt auch der BGH dabei eine umfassende Abwägung der wirtschaftlichen Interessen des Suchmaschinenbetreibers gem. Art. 16 GRCh, des Informationsinteresses der Öffentlichkeit sowie der Meinungs- und Pressefreiheit des Publizisten gem. Art. 11 GRCh mit dem Persönlichkeitsrecht des Betroffenen aus Art. 7 und 8 GRCh zugrunde. Dieses bewertet der BGH jedenfalls dort nicht als im Zweifel gewichtiger gegenüber den anderen betroffenen Interessen bzw. rechtlichen Belangen, wo es auch um das Grundrecht des dem Medienprivileg unterfallenden Inhalteanbieters gehe. In diesen Fällen seien alle sich gegenüberstehenden Grundrechte gleichrangig miteinander abzuwägen. Der BGH stützt sich dabei auf das BVerfG und modifiziert in gewisser Hinsicht die Rechtsprechung des EuGH, das den Persönlichkeitsschutz grundsätzlich etwas stärker gewichtet. Daher bleibt abzuwarten, ob und wie dieser sich dazu positioniert. Mittelbar betont der BGH den Schutz des Persönlichkeitsrechts jedoch wiederum, weil er aus der Gleichrangigkeit der betroffenen Interessen die Verpflichtung des Suchmaschinenbetreiber ableitet, im Falle eines Löschungsantrags nach Art. 17 DSGVO das beanstandete Suchergebnis stets umfassend daraufhin zu prüfen, ob es auf Inhalte verweist, an deren unbeschränkter Auffindbarkeit kein (überwiegendes) schützenswertes Interesse mehr besteht; seine frühere gegenteilige Rechtsprechung dazu hat der BGH ausdrücklich aufgegeben (Urt. Rn. 41).

36 Mit Beschluss vom 27. Juli 2020 – VI ZR 476/18 –[21] legte der BGH außerdem dem EuGH zwei Fragen zur Auslegung von Art. 17 DSGVO zur Vorabentscheidung vor. In diesem Verfahren wehrten sich die Kläger dagegen, dass die Suchmaschine etliche einige Jahre zurückliegende Presseartikel anzeigte, die sich kritisch mit den Geschäftsmodellen mehrerer Gesellschaften befassten, für die sie tätig waren. Die Berichte enthielten auch Fotos von ihnen, die neben den Suchergebnissen als Vorschaubilder (sog. „thumbnails“) angezeigt wurden. Der BGH hält insbesondere die Frage für entscheidungserheblich, ob es dem Betroffenen zuzumuten ist, die Wahrheit eines verlinkten Inhalts vorab – etwa im Rahmen des vorläufigen Rechtsschutzes – gerichtlich klären zu lassen, wenn der Löschungsanspruch allein davon abhängt, ob die Information zutraf (Beschluss Rn. 21 ff.). In Bezug auf die Vorschaubilder wiederum will der BGH klären lassen, ob die Abwägungsentscheidung über das Löschungsbegehren auch den Kontext des verlinkten Beitrags berücksichtigen muss, in dem das Bild veröffentlicht wurde, obwohl dieser Kontext in der Ergebnisanzeige nicht ersichtlich ist (Beschluss Rn. 46 ff.). Mit einer Entscheidung des EuGH über die beiden Vorlagefragen dürfte im Lauf des Jahres 2021 zu rechnen sein.

37 Schließlich hatte sich neben dem für datenschutzrechtliche Fragen zuständigen 6. Senat auch der Kartellrechtssenat des BGH mit einem datenschutzrelevanten Thema zu befassen. Auslöser war, dass das Bundeskartellamt am 6. Februar 2019 Facebook untersagt hatte, Nutzungsbedingungen weiterhin zu verwenden, auf deren Grundlage das Unternehmen personenbezogene Daten seiner Nutzer erfasst und über alle Facebook-Produkte hinweg miteinander verknüpft und verwendet. Da das OLG Düsseldorf auf Betreiben von Facebook

[21] https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=56be6f426fc1fafeff424140b38f701d&nr=110288&pos=0&anz=1

den Beschluss im Verfahren des vorläufigen Rechtsschutzes aussetzte, wurde die Untersagungsverfügung bislang jedoch noch nicht wirksam (s. dazu TB 2019, Rn. 70 ff.). Der BGH allerdings gab mit Beschluss vom 23. Juni 2020 – KVR 69/19 –[22] der Sache nach dem Bundeskartellamt recht. Danach kann der Betreiber eines sozialen Netzwerks sehr wohl seine marktbeherrschende Stellung missbrauchen, wenn er sich in den Nutzungsbedingungen ausbedingt, dem Nutzer ein „personalisiertes Erlebnis" bereitzustellen, für dessen Inhalt er solche personenbezogenen Daten verwendet, die er (auch) durch Erfassung des Aufrufs von Internetseiten außerhalb des sozialen Netzwerks gewinnt.

38 Die Entscheidung des BGH ist aus meiner Sicht außerordentlich zu begrüßen, da sie die „Marktrelevanz" personenbezogener Daten und das mit einer zunehmenden Datensammlung und -integration (von Facebook als „personalisiertes Erlebnis" verbrämt) verbundene Missbrauchspotential feststellt und damit den Boden dafür bereitet, dass datenschutzrechtliche Schutzziele auch mithilfe des Wettbewerbsrechts durchgesetzt werden können. Zurecht hat die Entscheidung des BGH (ebenso wie der ursprüngliche Beschluss des BKartA) daher auch international Aufsehen erregt. Sie verleiht den Bemühungen der EU-Kommission zur Verabschiedung eines „Digitale-Dienste-Gesetzes" (oben Rn. 10) zusätzliche Schubkraft.

39 Nach dem Beschluss des BGH gilt nun wieder die vierzehnmonatige Frist, die das BKartA Facebook gesetzt hatte, um den Betroffenen eine echte freie Wahlmöglichkeit einzuräumen: Sie müssen ihre Einwilligung in die Nutzung jener Daten verweigern oder widerrufen können, die Facebook aus anderen Quellen als der eigenen Plattform erhält; Nachteile dürfen sie dadurch nicht erleiden. Im übrigen bleibt, da es bisher „nur" um ein Eilverfahren ging, nun die Entscheidung in der Hauptsache abzuwarten, in der zunächst wieder das OLG Düsseldorf gefragt ist. Mit höchster Wahrscheinlichkeit wird sich anschließend erneut der BGH mit der Sache befassen müssen, möglicherweise – im Rahmen eines Vorabentscheidungsverfahrens – auch der EuGH, wenn es beispielsweise auf die Auslegung von Vorschriften der DSGVO oder von Art. 102 AEUV (Missbrauch einer marktbeherrschenden Stellung) ankommen sollte.

dd) Datenschutzprobleme

40 Die Corona-Pandemie hat die in Deutschland traditionell eher zögerlichen Bemühungen um eine **Digitalisierung und Flexibilisierung der Arbeitswelt** enorm beschleunigt. Hier entfaltet die Pandemie tatsächlich disruptive Kraft. Den vielen Vorteilen und Chancen stehen allerdings auch Risiken gegenüber. Zu ihnen zählt in datenschutzrechtlicher Hinsicht vor allem die Gefahr von Sicherheitslücken und -vorfällen sowie die zunehmende Abhängigkeit von marktbeherrschenden US-Konzernen und die mit ihr im Regelfall einhergehende Datenübermittlung in unsichere Drittstaaten. Für die erste Fallgruppe stehen beispielhaft die zahlreichen Cyberangriffe durch Schadprogramme wie Emotet, die schon im Vorjahr – wenngleich erfreulicherweise bislang nicht in meinem Zuständigkeitsbereich - zu massiven

[22] http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&client=12&pos=0&anz=1&Blank=1.pdf&nr=109506

Problemen führten (TB 2019, Rn. 82). Das Berliner Kammergericht etwa war fast ein halbes Jahr auf einen offline-Notbetrieb beschränkt und ist erst seit März 2020 wieder mit dem Berliner Landesnetz verbunden. Zur zweiten Fallgruppe gehören die erheblichen Schwierigkeiten, Videokonferenzen nicht nur gut handhabbar und komfortabel, sondern auch vollständig DSGVO-konform sicher durchzuführen (dazu unten Rn. 92 ff.). Auf welche Probleme dies bis in die höchste Ebene hinein stößt, wurde beispielsweise im November 2020 deutlich, als es einem niederländischen Journalisten ohne größeren Aufwand gelungen war, sich in eine vertrauliche Videokonferenz der europäischen Verteidigungsminister einzuschalten[23].

41 Die zunehmende Digitalisierung führt außerdem zu einer immer stärkeren Vernetzung unterschiedlichster Lebensbereiche und Endgeräte. Wenn unter diesen Bedingungen etwa – wie Mitte Dezember 2020 - die Suchmaschine von Google infolge einer gravierenden technischen Störung für einige Zeit ausfällt, dann kann dies dazu führen, dass parallel nicht nur andere Google-Dienste wie das Mailprogramm (Gmail), der Cloud-Speicher (Google Drive), die Navigation (Google Maps), der AppStore (Android Play Store) oder der Kalender nicht erreichbar bzw. verwendbar sind, sondern unvermittelt auch das „Smart Home" nicht mehr steuerbar ist[24]. Und wenn mangels sonstiger Möglichkeiten zur Freizeitgestaltung der Absatz moderner Fernsehgeräte in die Höhe schnellt, dürfte keineswegs allen Nutzern bewusst sein, dass der Komfort ihres ans Internet angeschlossenen SmartTV mit umfangreichen Datenübermittlungen an unterschiedlichste Unternehmen einhergehen kann, die womöglich Rückschlüsse auf das Seh- und Konsumverhalten, Neigungen und Interessen sowie viele andere persönliche Merkmale erlauben.

42 Ebenso instruktiv wie bedenklich sind vor diesem Hintergrund die Ergebnisse eines Berichts zur **Sektoruntersuchung Smart-TVs**[25], den das Bundeskartellamt im Juli 2020 veröffentlicht hat. Ihm liegt zwar, der Aufgabenstellung des BKartA entsprechend, der verbraucherschutzrechtliche Blickwinkel zugrunde. Aber einer der wesentlichen – und zunehmend bedeutsamer werdenden (oben Rn. 38) – Aspekte wirksamen Verbraucherschutzes sind die datenschutzrechtlichen Probleme und Konsequenzen des Geschäfts mit den personenbezogenen Daten, denen sich das BKartA in dem Bericht deshalb eingehend widmet. Im Ergebnis verarbeiten die Smart-TV-Hersteller selbst zwar nach den Feststellungen des BKartA in erster Linie gerätebezogene Basisdaten und nur in geringerem Umfang Nutzungsdaten. Sensiblere personenbezogene Daten allerdings sind in dem Moment betroffen, in dem der Nutzer Zusatzdienste (wie etwa einen Sprachassistenten) oder (Dritt-)Apps aktiviert. Hier geht es dann um Datenübermittlungen an unterschiedlichste sonstige Unternehmen wie etwa TV-Portal-Betreiber, Anbieter von Apps (z.B. Streamingdienste) oder elektronischen Empfehlungsdiensten. Das BKartA rügt insoweit nicht nur die pauschalen, oft kaum verständlichen und inhaltlich nicht ausreichenden oder unzutreffenden Datenschutzerklärungen. Sondern es weist auch darauf hin, dass die datenschutzbezogene Haftung des Herstellers für die Handlungen dieser unterschiedlichen Akteure – im datenschutzrechtlichen Sinne also die (jeweilige) Verantwortung - bislang völlig ungeklärt ist.

---

23 https://www.bbc.com/news/world-europe-55027641

24 https://www.bbc.com/news/technology-55299779

25 Sektoruntersuchung_SmartTVs_Bericht.pdf;jsessionid=9B4B233172DBDC26F91544E48E6926BA.2_cid362 (bundeskartellamt.de)

43 Mit dem umgekehrten Anliegen, nämlich den Anforderungen an eine DSGVO-konforme **Anonymisierung** personenbezogener Daten, befasst sich ein „Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche“[26], das der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI Bund) im Juni 2020 veröffentlichte. Grundlage war ein für diesen Zweck erstmals durchgeführtes öffentliches Konsultationsverfahren, in dem alle Interessierten – zu denen in diesem Falle auch andere Datenschutzbehörden gehörten - zum Thema Stellung nehmen konnten. Im Gegensatz zu pseudonymisierten Daten, die unter bestimmten Voraussetzungen „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“ (Art. 4 Nr. 5 DSGVO) setzt eine wirksame Anonymisierung voraus, dass der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann. Allerdings können sich die technischen und sonstigen Voraussetzungen für eine solche Wiederherstellbarkeit verändern. Daher kann „Anonymisierung“ letztlich nur ein vorübergehender oder relativer Zustand sein. Abgesehen davon setzt sie ihrerseits die Verarbeitung personenbezogener Daten voraus und bedarf deshalb einer eigenen Rechtsgrundlage. Nach der Einschätzung des BfDI Bund kommt dafür insbesondere der Tatbestand der kompatiblen Weiterverarbeitung (Art. 6 Abs. 4 DSGVO in Verbindung mit der ursprünglichen Rechtsgrundlage für die Datenverarbeitung) sowie die Erfüllung einer rechtlichen Verpflichtung gem. Art. 6 Abs. 1 lit. c) DSGVO in Betracht. Auch könne der Verantwortliche eine ihm obliegende Verpflichtung, die personenbezogenen Daten zu löschen, durch deren Anonymisierung erfüllen. Allerdings müsse er vor einer solchen Maßnahme in der Regel eine Datenschutz-Folgenabschätzung durchführen, Art. 35 DSGVO.

44 Schließlich sei hier noch auf den Abschlussbericht eines im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz durchgeführten Forschungsvorhabens zum „Innovativen Datenschutz-Einwilligungsmanagement“[27] hingewiesen, der im September 2020 veröffentlicht wurde. Eine wirksame Einwilligung in die Verarbeitung personenbezogener Daten muss die aus der DSGVO (insbes. Art. 6 Abs. 1 lit. a), Artt. 7 und 8) und der Rechtsprechung des EuGH hervorgehenden Anforderungen erfüllen. Insbesondere muss sie daher informiert, differenziert und freiwillig abgegeben worden sein (dazu Studie S. 19 ff.). Um dies gewährleisten zu können, muss der Verantwortliche ein geeignetes Einwilligungs-Managementsystem einsetzen. Der Bericht analysiert bereits vorhandene Modelle solcher Systeme im Online-Kontext (S. 51 ff.), wertet empirische Abfragen zur Erwartung der Verbraucher dazu aus (S. 88 ff.) und entwickelt Handlungsempfehlungen zur rechtskonformen und nutzerfreundlichen Einwilligung in Form eines Best Practice-Modells (S. 126 ff.). Unter anderem befasst sich die Studie in einem Exkurs auch mit der in der Praxis besonders bedeutsamen, aber auch umstrittenen Cookie-Einwilligung (S. 77 ff.).

45 Wenig überraschend gehört zu den Ergebnissen der Studie, dass Nutzer jene Anbieter, die ein differenziertes und leicht verständliches Einwilligungsmodell einsetzen, als wesentlich vertrauenswürdiger einschätzen als solche, die ihnen insoweit keine Wahlmöglichkeiten

[26] Positionspapier-Anonymisierung

[27] https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1

lassen. Aus verhaltenswissenschaftlicher Sicht wird ein Einwilligungssystem jedenfalls dann als nutzerfreundlich bewertet, wenn es die folgenden Anforderungen erfüllt: Es

- unterstützt die Wahlfreiheit und erlaubt Einstellungsmöglichkeiten,
- setzt keine oder lediglich datensparsame Voreinstellungen,
- vermeidet eine manipulierende Gestaltung,
- lenkt nicht vom Wesentlichen ab und vermeidet irreführendes Framing,
- setzt Visualisierungen allenfalls ein, soweit sie nicht ablenken und
- bietet zusätzliche Informationen und Hilfe nur im notwendigen Umfang an.

46 Allerdings gibt es nach Aussage der Studie bislang erst wenige Modelle, die tatsächlich jede dieser Anforderungen erfüllen. Umso mehr werden die Nutzer ein vorbildliches Einwilligungssystem als positives Distinktionsmerkmal wahrnehmen, das Glaubwürdigkeit und Seriosität des Anbieters vermittelt bzw. bekräftigt. Daher sollten sich auch die Rundfunkanstalten und ihre Beteiligungsunternehmen dort, wo sie eine Einwilligung zur Datenverarbeitung (auf ihrer Website) einholen, am Best Practice-Modell orientieren.

c Sonstiges

47 Seit 2017 verleiht eine Gemeinschaft mehrerer Organisationen, darunter die Datev Stiftung Zukunft, der Berufsverband der Datenschutzbeauftragten und die von den Landesmedienanstalten aus Rheinland-Pfalz und Nordrhein-Westfalen getragene EU-Initiative Klicksafe den Datenschutz Medienpreis (DAME). Prämiert werden Beiträge, die Datenschutz anschaulich und verständlich erklären und dabei zugleich die Themen und Sprache ihrer Zielgruppe treffen. Im Jahr 2019 war die Reportage eines Kölner Youtubers zum Thema „Das weiß das Internet über Dich!“ erfolgreich. Immerhin wurden daneben zwei öffentlich-rechtliche Sendungen mit einem Sonderpreis in Höhe von jeweils 1.500 Euro ausgezeichnet: Zum einen als „Bester Beitrag Hörfunk“ die Reportage „Tracking: Ein Tag im Internet – welche Spuren hinterlasse ich“ von Christian Schiffer, die Bayern 2 ausgestrahlt hatte, und zum anderen in der Kategorie „Comedy und Satire“ der Beitrag „Facebook in Real Life“ von Jakob Leube und Freddy Radeke für das NDR-Satire-Magazin „Extra 3“.

48 Die Verleihung des DAME ist ein sehr unterstützenswertes Mittel, Aufmerksamkeit für Datenschutzthemen zu erzeugen, und zwar gleich in doppelter Hinsicht: in bzw. bei den Medien sowie in der Bevölkerung, also bei den potentiell Betroffenen. 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.

49 Mit Blick auf seine enorme, stetig zunehmende Bedeutung für jeden Einzelnen wie auch die Gesellschaft insgesamt gehört das Thema Datenschutz spätestens seit dem Inkrafttreten der DSGVO nach meinem Verständnis aber ohnehin zum Kanon der Kernthemen, denen der öffentlich-rechtliche Rundfunk in seiner Berichterstattung besonderes Augenmerk widmen sollte. Zwar finden einschlägige Aspekte, wie die beiden prämiierten Beiträge zeigen, durchaus immer wieder und in unterschiedlichsten Sendungen und Formaten Platz.

Allerdings sind sie in den jeweiligen Programmen oder auch Online bisher weder inhaltlich-strukturell noch gar senderübergreifend erschlossen und daher in den Mediatheken allenfalls über die Suchfunktion als „Einzelprodukt" auffindbar (siehe auch den Hinweis auf die Mediatheken auf meiner Website)[28]. Für das an diesem Thema interessierte Publikum wäre es beispielsweise ein erheblicher Mehrwert, wenn die Rundfunkanstalten in ihren Onlineangeboten bzw. Mediatheken 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.

50 Solche Überlegungen liegen auch deshalb nahe, weil die Rundfunkanstalten selbst infolge der diversifizierten Ausspiel- und Kommunikationswege zunehmend in datenschutzrechtlich besonders sensiblen Umgebungen bzw. auf problematischen Plattformen präsent sind und sie dadurch nicht zuletzt auch aufwerten. Dies mag aus Gründen der publizistischen Wettbewerbsfähigkeit nachvollziehbar und berechtigt sein. Aber gerade deshalb sollten die Rundfunkanstalten das auf diesen Wegen angesprochene Publikum auch über die damit verbundenen datenschutzrechtlichen Konsequenzen aufklären, und zwar zielgruppengerecht und im Idealfall unter Einsatz der ihnen dafür zur Verfügung stehenden vielfältigen medialen Mittel. Besonders begrüßen würde ich dahingehende Bemühungen im und für das ARD/ZDF-Jugendangebot „funk", weil es hauptsächlich auf die Nutzung von Drittplattformen setzt. Für seine Zielgruppe stellen sich datenschutzrechtliche Fragen deshalb in besonderem Maße (s. zu alldem bereits TB 2019, Rn. 174 f.).

2 Der Gemeinsame Rundfunkdatenschutzbeauftragte

51 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. Allein 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. Dies verhindert, dass – anders als vor Inkrafttreten der DSGVO - der datenschutzrechtlich Verantwortliche (Intendant) bei der Besetzung der Aufsichtsposition formell mitwirkt.

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

[28] https://www.rundfunkdatenschutz.de/infothek/

a Allgemeine Entwicklung

53 Das in jeder Hinsicht beherrschende Thema des vergangenen Jahres war die Corona-Pandemie. Sie hat sich selbstverständlich auch auf meine Aufsichtstätigkeit ausgewirkt. Erfreulicherweise allerdings nur mittelbar: einen Krankheitsfall hatten wir in unserem kleinen Team nicht zu verzeichnen. Wohl aber einen – auf einen anderen Anlass zurückzuführenden - Personalwechsel: nach nur einem Jahr folgte meine Referentin aus sehr verständlichen Gründen einem Angebot des rbb, ihre dort bislang (parallel zu ihrer Teilzeitbeschäftigung in meiner Dienststelle) nur zu 50% wahrgenommene Aufgabe ab Mai in Vollzeit auszuüben, nachdem der rbb die Stellenkapazität entsprechend erhöht hatte. Glücklicherweise gelang es mir, trotz der durch die Restriktionen erschwerten Bedingungen und der konstruktionsbedingt unvermeidlichen Befristung die Stelle sofort nachzubesetzen.

54 Etwas überraschend waren die Auswirkungen des Pandemiegeschehens auf das Aufkommen an Beschwerden und sonstige aufsichtsrechtliche Angelegenheiten: Entgegen meiner Erwartung ging die Zahl der konkreten Beschwerden im Vergleich zum Vorjahr etwas zurück, und mich erreichten auch vergleichsweise wenige Anliegen wegen dieses Themas (s. dazu auch unten Rn. 127 f.). Ich führe dies unter anderem darauf zurück, dass die Verantwortlichen in meinem Zuständigkeitsbereich offenbar von ihren internen Datenschutzbeauftragten ausreichend und qualifiziert beraten wurden, sodass das Gros der entsprechenden Fragen ohne Rückversicherung bei der Aufsicht geklärt werden konnte.

55 Auf die Abläufe und Tätigkeiten in meiner Aufsichtsbehörde wirkte sich die Pandemie ebenfalls deutlich weniger aus, als ich befürchtet hatte. Das war in erster Linie auf den glücklichen Umstand zurückzuführen, dass es uns nach einem außerordentlich zähen Vorlauf gelungen war, den Bürobetrieb zum Beginn des neuen Jahres endlich auf ein elektronisches Aktenverwaltungssystem umzustellen – gerade noch rechtzeitig vor Beginn der staatlichen Restriktionen. Dies versetzte uns in die Lage, relativ zügig eine nahezu vollständige Abwicklung vom heimischen Arbeitsplatz aus zu organisieren, in der überwiegend ich die nötige Basispräsenz im Büro gewährleistete. Für die neue Kollegin, die uns seit Mai unterstützt, waren allerdings zunächst noch etliche technische Hürden zu überwinden. Nach einigen Wochen war aber auch sie weitestgehend von zuhause aus arbeitsfähig.

56 Im übrigen führten die Umstände jedoch dazu, dass Zeitabläufe und Terminplanungen anzupassen waren und Vor-Ort-Termine in den Rundfunkanstalten oder deren Gremien aufgeschoben bzw. durch Telefon- oder Videoschaltkonferenzen ersetzt werden mussten. Dies wirkte sich beispielsweise auf den Ablauf und den Umfang des Audits zum Verzeichnis der Verarbeitungstätigkeiten aus, das ich kurz vor dem Beginn der Corona-Pandemie eingeleitet hatte (unten Rn. 136 ff.). Für die Prüfung oder Erörterung bestimmter Themen und Vorhaben ist die Präsenz vor Ort gerade auch in aufsichtsrechtlicher Hinsicht hilfreich oder sogar nötig; der Einsatz der modernen elektronischen Kommunikationssysteme ermöglicht vieles, kann aber nicht alles ersetzen. Dazu zählt auch der zumindest gelegentliche persönliche Austausch mit den internen Datenschutzbeauftragten, den Mitgliedern der RDSK oder anderen Ansprechpartnern, ebenso wie der Besuch einschlägiger Fachveranstaltungen oder Fortbildungsangebote. Diese sind im vergangenen Jahr leider fast vollständig entfallen (unten Rn. 70). Auch der Zugang zur Bibliothek der nahegelegenen Juristischen Fakultät der Universität Potsdam oder zu den Bibliotheken der beiden Berliner Uni-

versitäten, auf den ich infolge des bisherigen Verzichts auf den Aufbau einer eigenen Fachbibliothek grundsätzlich angewiesen bin, war stark eingeschränkt.

57 Im übrigen gilt weiterhin, dass ich mich angesichts der ausgesprochen knappen Ressourcen (s. TB 2019, Rn. 115 f.) grundsätzlich auf die folgenden Aufgaben aus dem umfangreichen Katalog des Art. 57 Abs. 1 DSGVO konzentrieren muss, von denen ich mich wiederum nur einigen im Jahr 2020 tatsächlich 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).

b Zusammenarbeit in der RDSK

58 Wie bereits berichtet, hat sich im Jahr 2019 als Zusammenschluss der Datenschutzstellen mit Aufsichtsfunktion im öffentlich-rechtlichen Rundfunk die Rundfunkdatenschutzkonferenz (RDSK) konstituiert (TB 2019, Rn. 129 f.). Noch befindet sie sich in der „Entwicklungsphase", und gerade deshalb wirkte es sich für dieses noch junge Gremium nachteilig aus, dass 2020 eine persönliche Zusammenkunft nicht möglich war. In zwei Schaltkonferenzen und im übrigen im schriftlichen Verfahren konnten in diesem Kreis gleichwohl einige Grundlagen geklärt und Positionen abgestimmt werden. Ein wesentliches Anliegen ist mir nach wie vor eine hinreichend klare Abgrenzung zum Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AKDSB). Diesem gehören außer mir alle anderen Mitglieder der RDSK an, darüber hinaus die internen Datenschutzbeauftragten der fünf Rundfunkanstalten in meinem Zuständigkeitsbereich, des Beitragsservice sowie weiterer Gemeinschaftseinrichtungen, von ARTE Deutschland und des ORF. Der Aufgabenzuordnung von Art. 39 DSGVO folgend, sehe ich im AKDSB das zentrale Gremium, das die Rundfunkanstalten auf der operativen Ebene in deren datenschutzrelevanten Angelegenheiten berät. Demgegenüber zeigt die RDSK mit Blick auf Art. 57 DSGVO aus der aufsichtsrechtlichen Perspektive zu wichtigen Themen Auslegungsoptionen und -grenzen auf, formuliert Handlungsanweisungen oder -empfehlungen und positioniert sich in mediendatenschutzrechtlichen Fragen.

59 Um die RDSK auch im Außenverhältnis sichtbarer zu machen, soll sie eine eigene Homepage erhalten, über die dann zusätzlich zu den bestehenden Möglichkeiten (etwa über meine Infothek) unter anderem die Regularien, Beschlüsse und Positionspapiere abrufbar sein werden. Die entsprechenden Vorbereitungen konnten 2020 noch nicht ganz abgeschlossen werden. Abgestimmt ist jedoch bereits ein eigenes Logo, das dann künftig auch die Homepage sowie die Veröffentlichungen der RDSK kennzeichnen wird.

60 Außerdem verständigten sich die Mitglieder der RDSK auf zwei von mir vorbereitete Verwaltungsvereinbarungen, die die Wahrnehmung der **Datenschutzaufsicht über Gemeinschaftseinrichtungen** der Rundfunkanstalten sowie über deren **gemeinsame Beteiligungsgesellschaften** regeln. Da der Kreis der Beteiligten sich in beiden Fällen voneinander unterscheidet – nur die gesetzlich als Aufsichtsbehörde nach Art. 51 DSGVO bezeichneten Rundfunkdatenschutzbeauftragten sowie der Beauftragte für den Datenschutz der Deutschen Welle sind auch für die Aufsicht über Beteiligungsunternehmen der jeweiligen Rundfunkanstalt zuständig -, waren die damit verbundenen Fragen in zwei Regelwerken zu behandeln. Beiden liegt das Prinzip zugrunde, dass der jeweils Verantwortliche sich nur an das als federführend benannte RDSK-Mitglied wenden muss, um die ihm obliegenden Verpflichtungen etwa aus Art. 33 DSGVO zu erfüllen. Dieses wiederum handelt jeweils auch mit Wirkung für und gegen die anderen Aufsichtsstellen. Nur in bestimmten, besonders gewichtigen Fällen ist dort eine vorherige Abstimmung über einzelne Maßnahmen mit den anderen betroffenen RDSK-Mitgliedern vorgesehen. Dies soll den administrativen Aufwand auf Seiten der Verantwortlichen, aber auch im Kreis der RDSK auf das Nötige reduzieren.

61 Im übrigen hat sich die RDSK im Berichtszeitraum unter anderem mit den Konsequenzen der jüngeren Rechtsprechung für den Einsatz von Cookies zur Nutzungsmessung der Rundfunkanstalten (dazu unten Rn. 102 ff.) sowie zur Datenübermittlung in Drittstaaten (oben Rn. 29) befasst. Für die Jahre 2021 und 2022 bin ich zum Vorsitzenden gewählt worden.

c Zusammenarbeit mit sonstigen Aufsichtsbehörden

62 Der im Grunde erst 2019 verbindlich in Gang gekommene regelmäßige Austausch zwischen den in der DSK zusammengeschlossenen **staatlichen Datenschutzbeauftragten** sowie den weiteren, sogenannten „spezifischen" Aufsichtsbehörden ist leider 2020 umständehalber ein wenig ins Stocken geraten: Statt der an und für sich als Regel fest eingeplanten zwei Präsenztreffen konnte auf Einladung des letztjährigen Vorsitzenden der DSK, des Sächsischen Datenschutzbeauftragten, im Oktober 2020 nur eine kürzere Videoschaltkonferenz stattfinden. Im Mittelpunkt stand die Information über den Stand der Diskussion in der DSK zu etlichen relevanten Themen wie etwa die Konsequenzen aus dem Urteil des EuGH in Sachen „Schrems II" (oben Rn. 26 f.), zum Datenschutz bei der Bewältigung der Corona-Pandemie oder zum Einsatz von Videokonferenzsystemen. Für die Runde der an diesem Austausch beteiligten Aufsichtsstellen gilt ähnliches wie für die RDSK: Sie befindet sich noch in der „Findungsphase". Ein gemeinsames Verständnis vom Sinn und Zweck dieses Austauschs ist erfahrungsgemäß viel leichter bei persönlichen Zusammenkünften als im Rahmen von (Video-)Schaltkonferenzen zu entwickeln, umso mehr, als auch der Teilnehmerkreis nicht immer identisch ist. Immerhin scheint inzwischen aber ein gewisses wechselseitiges Grundverständnis geschaffen. Ich gehe deshalb optimistisch davon aus, dass die mittlerweile vorhandene Basis stabilisiert und spätestens dann weiter ausgebaut werden kann, sobald die pandemiebedingten Einschränkungen entfallen sind.

63 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 Februar 2020 an einer Präsenzsitzung sowie im Oktober 2020 an einer Videoschaltkonferenz 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. Unbeschadet des Umstands, dass der Gaststatus eine förmliche Beteiligung an der Meinungsbildung im AK naturgemäß nicht vorsieht, nutze ich insoweit dann 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.

64 Außerdem war die RDSK – durch den Kollegen des NDR – auch bei Sitzungen des AK Medien der DSK im März und September 2020 sowie im Februar 2020 durch die Kollegin von Radio Bremen bzw. meine damalige Referentin auch im AK Technik vertreten. Da beide Kolleginnen im Frühjahr aus unterschiedlichen Gründen aus ihrer Funktion ausschieden und die Nachfolgefrage bis Ende des Jahres noch nicht geklärt werden konnte, wird sich erst 2021 herausstellen, ob und inwieweit die RDSK im AK Technik noch vertreten sein wird. Angesichts der – aufgabengemäß – sehr stark technikzentrierten Agenda ist diese Runde weitgehend mit den IT-Fachleuten der staatlichen Datenschutzaufsichten besetzt; entsprechende fachliche Expertise auf Seiten der RDSK brachte bis zu ihrem Ausscheiden lediglich meine frühere Referentin mit. Angesichts der großen Bedeutung von Technikgestaltung und -anwendung für einen wirksamen Datenschutz halte ich eine Vertretung der RDSK in diesem Gremium aber auf jeden Fall für sinnvoll. Gleiches gilt für den AK Datenschutz- und Medienkompetenz, an dem ich mich gern beteiligen würde, der allerdings offenbar nur sehr sporadisch – zuletzt im Herbst 2019 - tagt.

65 Weiterhin nicht abschließend beantwortet ist die Frage, ob und wie die DSK die Rundfunkdatenschutzbeauftragten in die Agenda des Europäischen Datenschutzausschusses (EDSA)[29] einbezieht (s. TB 2019, Rn. 142). Immerhin ist inzwischen geklärt, dass die Vorschriften des deutschen Rundfunkrechts, die auf der Basis von Art. 85 DSGVO die Datenschutzaufsicht im (öffentlich-rechtlichen) Rundfunk ausgestalten, bei der Europäischen Kommission notifiziert wurden. Damit sind etwaige letzte verbliebene formelle Zweifel daran, dass es sich bei den gesetzlich bzw. staatsvertraglich bestimmten Rundfunkdatenschutzbeauftragten um Aufsichtsbehörden nach Art. 51 DSGVO handelt, ausgeräumt. Demzufolge gibt es keinen Hinderungsgrund, die RDSK zumindest grundsätzlich in den Informationsaustausch auf nationaler Ebene einzubeziehen. Eine umfassende Beteiligung dürfte ohnehin weder sinnvoll noch leistbar sein. Wohl aber ist es wünschenswert, frühzeitig über die auf europäischer Ebene aktuell und künftig diskutierten Themen sowie das jeweils vorgesehene weitere Verfahren einschließlich des vorgesehenen Zeitpunkts für eine Beschlussfassung informiert zu sein. Nur dann hat die RDSK die Chance, sich zu relevanten

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

Themen wenigstens auf der nationalen Ebene gegenüber den deutschen Vertretern im Europäischen Datenschutzausschuss vorab zu äußern.

66 Auch eine Zusammenkunft der Mitglieder des sogenannten „Virtuellen Datenschutzbüros“[30] gab es im Jahr 2020 nicht. Dabei handelt es sich um eine von zahlreichen Datenschutzinstitutionen aus dem In- und deutschsprachigen Ausland getragene zentrale Online-Informations- und Anlaufstelle für Datenschutzfragen, an der ich seit 2019 beteiligt bin. Die Geschäftsführung obliegt dem Datenschutzzentrum Schleswig-Holstein; einige Punkte der dafür maßgeblichen Geschäftsordnung wurden im Berichtszeitraum im schriftlichen Verfahren aktualisiert. Über die Plattform sind unter anderem Beiträge, Tätigkeitsberichte oder Presseinformationen der verschiedenen Projektpartner abrufbar.

67 Jenseits solcher formellen Anlässe habe ich auch im vergangenen Jahr wieder den Kontakt und Austausch mit anderen Aufsichtsstellen – insbesondere mehreren Landesdatenschutzbeauftragten - auf der bilateralen Ebene gepflegt. Leider waren umständehalber nur in einigen wenigen Fällen persönliche Verabredungen möglich. In jedem Falle aber erweist es sich als sinnvoll, beidseitig relevante Themen zu identifizieren und sich über die jeweiligen Sichtweisen oder Bewertungen auszutauschen. Dies gilt umso mehr, als es immer wieder vorkommt, dass sich Beschwerdeführer nur oder zusätzlich an die – in der Öffentlichkeit naturgemäß viel präsenteren – Landesdatenschutzbehörden auch in Angelegenheiten wenden, für die ich zuständig bin; zahlreiche Eingaben haben mich deshalb im Berichtsjahr erneut auf diesem Umweg erreicht. Gelegentlich „drohen“ Petenten mir gegenüber auch mit dem Gang zur vermeintlich übergeordneten Beschwerdeinstanz der Landesdatenschutzbeauftragten. Im Binnenverhältnis zu den für mich innerhalb meines Zuständigkeitsbereichs relevanten staatlichen Aufsichtsbehörden gab es ansonsten bislang keinerlei nennenswerte Differenzen oder sonstige Probleme; der bilaterale Austausch war durchweg konstruktiv und angenehm.

d Zusammenarbeit mit den internen Datenschutzbeauftragten

68 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, habe ich mittels zweier Videoschaltkonferenzen fortgeführt. Dies gibt den Kolleginnen und Kollegen die Möglichkeit, die für diesen Kreis insgesamt relevanten Vorgänge, mit denen sie jeweils befasst sind, in einer solchen Runde zur Diskussion zu stellen und gegebenenfalls eine Positionierung bzw. Klärung durch mich herbeizuführen. Umgekehrt erhalte ich selbst wichtige Hinweise auf aufsichtsrelevante Themen aus der betrieblichen Perspektive und informiere die Runde über Erfahrungen und Vorhaben aus meiner Aufsichtspraxis.

69 Insgesamt empfinde ich die Zusammenarbeit sowohl in diesem Kreis insgesamt wie auch jeweils bilateral als kooperativ und offen. Leider waren auch hier persönliche Treffen die Ausnahme, da mir jeweils nur ein Vor-Ort-Termin in den Rundfunkanstalten im Rahmen des Audits (unten Rn. 136 ff.) möglich war. In unterschiedlicher Ausprägung beschäftigt al-

[30] https://www.datenschutz.de/

le Mitglieder dieser Runde die Konkretisierung ihrer Rechte und Pflichten im Verhältnis zum jeweils Verantwortlichen bzw. den mit datenschutzrelevanten Aufgaben befassten Fachbereichen, zumal die DSGVO insoweit im Vergleich zur früheren Rechtslage durchaus die eine oder andere Veränderung bewirkt hat (s. dazu bereits TB 2019, Rn. 204 ff., 211 ff.). Klärungsbedarf zeigte sich insoweit teilweise nicht nur in Bezug auf die Zuständigkeit für rechtlich unselbstständige Organisationseinheiten mehrerer gemeinsam Verantwortlicher (Gemeinschaftseinrichtungen), die eine Rundfunkanstalt für diese Gemeinschaft organisatorisch-administrativ betreut, sondern auch funktional etwa im Verhältnis zu den Organen und bestimmten sonstigen der Rundfunkanstalt zugehörigen oder angegliederten Organisationseinheiten. Konkrete Beschwerden bzw. Streitfälle dazu haben mich allerdings im Berichtszeitraum nicht erreicht.

e Sonstiges

70 Für fachliche Aktivitäten jenseits der Aufsichtsfunktion im engeren Sinne, namentlich den Besuch einschlägiger Vortrags- oder Fortbildungsveranstaltungen boten sich im Jahr 2020 kaum Gelegenheiten, da die meisten ersatzlos entfielen. Lediglich an einer von der Stiftung Datenschutz in Berlin organisierten Podiumsdiskussion zur Zukunft der Datenschutzaufsicht habe ich teilgenommen. Hintergrund waren die unter anderem von der Datenethikkommission angestoßenen Überlegungen zu einer weitergehenden Bündelung der Datenschutzaufsicht für den privatwirtschaftlichen Bereich beim BfDI Bund.

3 Schwerpunktthemen der eigenen Praxis

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

a Auskunftsverfahren

72 Bei weitem die meisten aller bei mir eingegangen Anfragen und Beschwerden betreffen das Recht auf Auskunft gemäß Art. 15 DSGVO. Davon entfiel wiederum der mit Abstand größte Anteil auf den Beitragsservice von ARD, ZDF und Deutschlandradio. Freilich löste nur ein Teil davon aufsichtsrechtliche Verfahren aus: Häufig hatten die Petenten verkannt, dass sich der Anspruch nicht an die Aufsicht, sondern an den jeweils Verantwortlichen richtet, an den ich insoweit dann verwiesen habe. Entsprechendes galt für mehrere Beschwerden von Rundfunkteilnehmern außerhalb meines Zuständigkeitsbereichs, die ich an das jeweilige RDSK-Mitglied bzw. in einem Fall an die Berliner Landesdatenschutzbeauftragte verwiesen habe. Umgekehrt haben mich zahlreiche Beschwerden – nicht nur, aber vor allem in Bezug auf Auskunftsbegehren – auf dem Umweg über eine staatliche Datenschutzaufsichtsbehörde erreicht, da die rundfunkspezifische Datenschutzaufsicht vielfach unbekannt ist.

73 In etlichen Fällen monierten die Petenten, dass sie die geforderte Auskunft nicht oder nicht innerhalb der von Art. 12 Abs. 3 DSGVO vorgegebenen **Monatsfrist** erhalten hätten. Insgesamt trat dieser Beschwerdegrund aber deutlich weniger auf als im Vorjahr; insofern haben sich offenkundig die vom Beitragsservice auf meine Veranlassung hin im Jahr 2019 durchgeführten Korrekturen und Optimierungen der technischen und organisatorischen Vorgaben für die Erfassung datenschutzrechtlich relevanter Eingänge und deren interne Abwicklung positiv bemerkbar gemacht. Mehrfach war eine Fristüberschreitung auf ein Versagen im Einzelfall, nicht auf systemische Probleme zurückzuführen. Bei der Bewertung habe ich in Rechnung gestellt, dass das vom Beitragsservice zu bewältigende enorme Korrespondenzaufkommen gerade angesichts der pandemiebedingt erschwerten Arbeitsbedingungen alle Beteiligten besonderen Belastungen aussetzt: allein im ersten Quartal 2020 gingen dort, zusätzlich zum eigentlichen Geschäftsverkehr in Gestalt der Zuschriften in Beitragsangelegenheiten, rund 25.000 Auskunftsbegehren nach Art. 15 Abs. 1 DSGVO ein.

74 Gleichwohl habe ich dem Beitragsservice gemäß Art. 58 Abs. 2 lit. d) DSGVO aufgegeben, seine Verfahrensabläufe und Verhaltensvorgaben noch einmal dahingehend zu prüfen und zu optimieren, dass entsprechende Versäumnisse künftig nach Möglichkeit ausgeschlossen sind. Der Beitragsservice hat mich innerhalb der dafür eingeräumten Frist über die daraufhin ergriffenen unterschiedlichen Maßnahmen informiert. Seither hat mich keine begründete Beschwerde über eine nicht oder zu spät erteilte Auskunft des Beitragsservice mehr erreicht.

75 Der Vollständigkeit halber sei angemerkt, dass Art. 12 Abs. 3 S. 2 DSGVO dem Verantwortlichen die Möglichkeit gibt, die Monatsfrist nach S. 1 um bis zu zwei Monate zu verlängern, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Davon kann natürlich auch der Beitragsservice Gebrauch machen. Allerdings entbindet dies den Verantwortlichen nicht davon, das Auskunftsbegehren überhaupt formell als solches zu erfassen und innerhalb der Monatsfrist darauf zu reagieren. Denn nach S. 3 hat er die betroffene Person innerhalb dieses Zeitraums zumindest über die Fristverlängerung und die dafür maßgeblichen Gründe zu informieren.

76 Eine der bei mir eingegangenen Auskunftsbeschwerden erwies sich als begründet, obwohl das Fristversäumnis weniger auf ein wie auch immer geartetes Versäumnis des Beitragsservice als vielmehr auf die besonderen Umstände des Einzelfalls zurückzuführen war. Denn den Antrag auf Auskunft nach Art. 15 DSGVO hatte der Inhaber einer auf seinen Namen firmierenden Gesellschaft bürgerlichen Rechts (GbR) gestellt, für die der Beitragsservice mit Blick auf die einschlägigen Vorschriften des RBStV ein Beitragskonto als juristische Person angelegt hatte. Da den datenschutzrechtlichen Auskunftsanspruch aber nur natürliche, nicht jedoch juristische Personen geltend machen können, war der Beitragsservice zunächst davon ausgegangen, dass er insoweit nicht tätig werden müsse. Tatsächlich aber muss in Fällen wie diesen, in denen die Firma der GbR oder einer anderen juristischen Person aus einem oder mehreren Namen natürlicher Personen besteht, der Auskunftsanspruch greifen, denn hier ist die Firmenbezeichnung selbst bereits ein personenbezogenes Datum. Dementsprechend hat der Beitragsservice aus Anlass dieses Beschwerdefalls intern klargestellt, dass in derartigen Fällen auch gegenüber dem Firmeninhaber einer juristischen Person Auskunft zu erteilen ist.

77 Eine besondere Herausforderung besteht für den Beitragsservice darin, die Auskunft so **verständlich und vollständig** wie möglich zu erteilen. Denn nach Art. 12 Abs. 1 DSGO ist der Verantwortliche verpflichtet, der betroffenen Person die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in klarer und einfacher Sprache zu übermitteln. Insoweit beschwerte sich ein Petent bei mir darüber, dass der Beitragsservice in der Auskunft lediglich pauschal handels- und steuerrechtliche Aufbewahrungspflichten erwähne, ohne diese im einzelnen zu erläutern bzw. zu begründen. Gleiches gelte für Hinweise auf regelmäßige Löschroutinen und ein Löschkonzept sowie die Vorgaben für interne Zugriffsberechtigungen.

78 Dazu ist zunächst festzustellen, dass weder aus Art. 12 Abs 1 DSGVO noch aus den einschlägigen Erwägungsgründen der DSGVO hervorgeht, was im einzelnen unter den Begriffen "präzise", "transparent", "verständlich" und/oder "klare und einfache Sprache" zu verstehen sein soll. Dies wiederum liegt daran, dass es angesichts der äußerst unterschiedlichen und unterschiedlich komplexen Sachverhalte überhaupt nicht möglich ist, abstrakt und generell vorzugeben, wie eine diesen Anforderungen entsprechende Information bzw. Auskunft auszusehen hätte. Im allgemeinen wird sich der Maßstab insoweit am Verständnis eines durchschnittlichen Adressaten orientieren. Dabei muss der Verantwortliche die Möglichkeit haben, den für eine Information bzw. eine Auskunft aufzuwendenden Aufwand in einem vernünftigen Verhältnis zwischen allgemeiner Umschreibung und einzelfallbezogener Umsetzung zu halten, also zwischen einer Wiedergabe der abstrakten bzw. allgemeinen datenschutzrechtlichen Vorkehrungen in seinem Verantwortungsbereich und einer Darstellung der daraus für den jeweiligen Einzelfall folgenden Konsequenzen. Insgesamt gesteht die DSGVO insoweit dem Verantwortlichen einen erheblichen Gestaltungsspielraum zu. Er dürfte erst und nur dann verletzt sein, wenn die Information bzw. die erteilte Auskunft grob ungenau, weitgehend unverständlich oder irreführend ist.

79 Allerdings bleibt dann noch offen, unter welchen Voraussetzungen dem Verantwortlichen eine solche konkrete Angabe der Aufbewahrung einzelner personenbezogenen Daten im Sinne von Art. 15 Abs. 1 lit. d) DSGVO „nicht möglich“ ist. Der Beitragsservice verweist insoweit auf den mit einer individualisierten Aussage verbundenen enormen Bearbeitungsaufwand. Angesichts der unüberschaubaren Vielzahl an Beitragskonten sowie unterschiedlichster Unterlagen und Daten kann ich dies grundsätzlich nachvollziehen. Letztlich geht es um einen Ausgleich des Interesses der betroffenen Person an einer möglichst individuellen und konkreten Auskunft mit dem Interesse des Beitragsservice (das letztlich dem Interesse aller Beitragszahler entspricht), den damit verbundenen Aufwand auf ein vertretbares Maß zu beschränken. Daher halte ich es grundsätzlich beispielsweise für statthaft, die in großer Zahl eingehenden und nicht selten auf vorgefertigte Musterschreiben zurückgehenden Auskunftsbegehren in einem weitgehend automatisierten, zweistufigen Verfahren zu beantworten (s. bereits TB 2019, Rn. 152 f.). Auch kann angesichts der Komplexität der unterschiedlichen Beitragssachverhalte der Beitragsservice nicht gezwungen sein, die Aufbewahrungsfristen für jedes einzelne personenbezogene Datum zu benennen und zu begründen. Ebenso wenig ist er verpflichtet, die für die Aufbewahrung einzelner Daten bzw. Unterlagen maßgeblichen, ihrerseits nicht selten komplexen und anspruchsvollen gesetzlichen Regelungen im einzelnen zu erläutern bzw. so zu übersetzen, dass sie für jede interessierte Person ohne weiteres verständlich sind. Entsprechendes gilt schließlich für die in-

ternen organisatorischen Maßnahmen, mithilfe derer der Verantwortliche die ihm obliegenden gesetzlichen Verpflichtungen umsetzt.

80 In dem betreffenden Beschwerdeverfahren ging es jedoch um ein bereits abgemeldetes, also in sich abgeschlossenes Beitragskonto. Dies warf für mich die Frage auf, ob der Beitragsservice nicht zumindest in solchen Fällen eine individualisierte Auskunft über die verbleibende konkrete Aufbewahrungsdauer der dort gespeicherten personenbezogenen Daten zu erteilen hat. Denn grundsätzlich muss der Verantwortliche spätestens mit Abschluss eines bestimmten Vorgangs, der mit der Verarbeitung personenbezogener Daten verbunden ist, ohnehin den Zeitraum festlegen, an dessen Ende diese Daten spätestens zu löschen sind. Andererseits sind die konkreten Aufbewahrungs- und Löschfristen von einer Vielzahl sonstiger Faktoren beeinflusst, die wiederum teilweise vom Verhalten der jeweils beitragspflichtigen Person – wie etwa weiterer Korrespondenz - abhängen. Diese Faktoren hat der Beitragsservice für jedes Beitragskonto im Rahmen eines mehrstufigen, iterativen Prüfverfahrens festzustellen und zu konkretisieren sowie die daraus folgenden Vorgaben nach Anlass und Bedarf gegebenenfalls zu aktualisieren. Daher können sich konkrete Aufbewahrungs- und Löschfristen, abhängig von der Entwicklung eines Beitragssachverhalts bzw. – kontos, auch immer wieder verändern bzw. verschieben, während und obwohl die zugrunde liegenden gesetzlichen Regelungen unverändert bleiben.

81 Im Ergebnis war die Beschwerde daher im betreffenden Fall unbegründet. Unbeschadet dessen haben meine Anmerkungen und Hinweise den Beitragsservice veranlasst, seine Textbausteine zur Auskunft über die internen Aufbewahrungsregeln um einige Passagen zu ergänzen und zu präzisieren, die den Betroffenen zumindest Anhaltspunkte für die betreffenden Zeiträume sowie Hinweise auf die dafür maßgeblichen gesetzlichen Vorschriften geben.

b Beitragsbescheid und Art. 22 DSGVO

82 In einem Beschwerdeverfahren hatte ich der Frage nachzugehen, ob die Festsetzungsbescheide des Beitragsservice wie auch die Vollstreckungsersuchen der jeweiligen Landesrundfunkanstalt womöglich gegen Art. 22 DSGVO verstoßen. Nach dieser Vorschrift hat die betroffene Person „das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt." Der Adressat eines vollständig automatisiert erlassenen Festsetzungsbescheides bzw. belastenden Verwaltungsakts kann in diesem Sinne grundsätzlich einer Entscheidung unterworfen sein, die auf einer automatisierten Verarbeitung beruht.

83 Allerdings ist Art. 22 Abs. 1 DSGVO auf die beitragsrechtlichen Festsetzungsbescheide nicht anwendbar. Bei diesen handelt es sich um sogenannte gebundene Verwaltungsakte: Die Voraussetzungen, unter denen die Pflicht zur Zahlung des Rundfunkbeitrags entsteht, ergeben sich unmittelbar aus dem Rundfunkbeitragsstaatsvertrag (RBStV). Der Beitragsservice prüft namens und im Auftrag der jeweils zuständigen Landesrundfunkanstalt mithilfe eines automatisierten Verfahrens lediglich, ob und ab wann die gesetzlichen Voraussetzungen der Beitragspflicht im jeweiligen Einzelfall vorliegen. Weder kann er dafür eige-

ne Kriterien zugrunde legen, noch hat er im Regelfall die Möglichkeit, von einer Feststellung der Beitragspflicht ganz oder teilweise abzusehen oder den sich aus dem festgestellten Sachverhalt ergebenden Zeitpunkt zu verändern. Nur dann aber wäre der Betroffene im Sinne des Art. 22 DSGVO einer automatisierten Entscheidungsfindung „unterworfen".

84 Darüber hinaus bewertet der Beitragsservice im Rahmen des Beitragsfestsetzungsverfahrens auch keine persönlichen Aspekte. Ist eine Person mit einer (beitragspflichtigen) Wohnung angemeldet, ohne den Rundfunkbeitrag zu entrichten, dann muss der Beitragsservice den Rundfunkbeitrag zwingend festsetzen. Auf derartige Sachverhalte ist Art. 22 DSGVO nicht anwendbar. Unabhängig davon hat der mit dem 23. Rundfunkänderungsstaatsvertrag mit Wirkung seit Oktober 2019 neu eingefügte § 10a RBStV nunmehr vorsorglich ausdrücklich klargestellt, dass die zuständige Landesrundfunkanstalt (und damit auch der in ihrem Auftrag handelnde Beitragsservice) „rundfunkbeitragsrechtliche Bescheide automatisiert erlassen (kann), sofern weder ein Ermessen noch ein Beurteilungsspielraum besteht."

85 Die Vollstreckungsersuchen der Landesrundfunkanstalten verstoßen schon deshalb nicht gegen Art. 22 DSGVO, weil es sich um rein behördeninterne Erklärungen ohne Außenwirkung im Verhältnis zur jeweils betroffenen Person handelt. Unabhängig davon erfüllen auch sie aus den bereits genannten Gründen ebenfalls nicht die Kriterien eines vollständig automatisiertes Behördenhandelns im Sinne von Art. 22 DSGVO.

86 Soweit die Landesrundfunkanstalt bzw. der in ihrem Auftrag handelnde Beitragsservice schließlich die personenbezogenen Daten des jeweiligen Beitragsschuldners an den zuständigen Vollstreckungsbeamten der Justizverwaltung übermittelt, ist dies nach Art. 6 Abs. 1 S. 1 lit. e) Alt. 1 DSGVO gerechtfertigt. Die Vollstreckung von Geldforderungen nach dem RBStV ist eine Aufgabe, die im öffentlichen Interesse liegt. Hierfür ist die Datenverarbeitung erforderlich. Insbesondere muss der Beitragsservice die Beitragsnummer des Betroffenen an die Vollstreckungsbeamten übermitteln, die sie benötigen, um mit der Rundfunkanstalt in der Vollstreckungsangelegenheit zu kommunizieren (s. auch unten Rn. 88).

c Meldedatenabgleich

87 In mehreren Beschwerdeverfahren hatte ich den Vorwurf zu überprüfen, der Beitragsservice habe seine Festsetzungsbescheide auf fehlerhafte personenbezogene Daten gestützt. Unabhängig davon, ob es sich dabei im Kern überhaupt um einen von der Datenschutzaufsicht und nicht vielmehr (im entsprechenden Verwaltungsstreitverfahren) beitragsrechtlich zu überprüfenden Sachverhalt handelte, stellte sich heraus, dass die fehlerhaften Daten dem Beitragsservice jeweils auf der Basis von Meldedatenübermittlungen (§ 11 Abs. 4, 5 RBStV) zugegangen waren. Auslöser war letztlich jeweils ein Versehen bei der zuständigen Meldebehörde. Da der Beitragsservice die ihm auf diesem Weg zugehenden Daten nicht selbst überprüfen kann, muss er sie seiner Korrespondenz mit den Beitragszahlern zunächst einmal zugrunde legen. Ein Verstoß gegen Datenschutzvorschriften liegt darin nicht. Wohl aber kann der Beitragsservice auf einen entsprechenden Antrag der betroffenen Person hin in solchen Fällen verpflichtet sein, die Daten zu berichtigen (Art. 16 DSGVO) oder zu löschen (Art. 17 DSGVO).

d Beitragsnummer

88 Der Beitragsservice richtet für jeden festgestellten Beitragssachverhalt ein sogenanntes Beitragskonto mit einer individuellen Nummer ein. Unter dieser wickelt er anschließend die gesamte Korrespondenz ab. In einigen Fällen bezweifelten Petenten, dass es zulässig sei, ein solches personenbezogenes Datum anzulegen, insbesondere da sie darüber - angeblich – nicht informiert worden seien. Datenschutzrechtlich ist dies allerdings nicht zu beanstanden. Dabei handelt es sich um ein internes Ordnungs- und Identifikationskriterium, auf das der Beitragsservice angesichts des enormen Korrespondenz- bzw. Datenaufkommens angewiesen ist, um sämtliche dort zu verarbeitenden Daten dem jeweils zutreffenden Beitragssachverhalt (Person bzw. Betriebsstätte) zuordnen zu können. Angesichts von mehr als 40 Millionen Beitragskonten ist der Beitragsservice aus datenschutzrechtlicher Sicht nicht nur berechtigt, sondern sogar verpflichtet, durch geeignete Vorkehrungen dafür zu sorgen, dass die dort zu einer Person verarbeiteten Daten auf ein entsprechendes Auskunftsersuchen hin ausschließlich dieser Person und nicht etwa einer namensgleichen oder unter derselben Anschrift wohnenden anderen Person übermittelt werden. Die Beitragsnummer ist ein geeignetes Mittel, um eine Personenverwechslung auszuschließen. Der Einsatz eines solchen Ordnungsinstruments liegt deshalb gerade auch in datenschutzrechtlicher Hinsicht im Interesse aller Beitragszahler, da dies die Gefahr einer fehlerhaften Datenverarbeitung verringert. Aus dem gleichen Grund greifen andere Behörden und Unternehmen ebenfalls auf entsprechende Hilfsmittel zurück. Daher bestehen auch keine Bedenken dagegen, dass der Beitragsservice die Beitragsnummer im Zusammenhang mit der Abwicklung von Beitragsverfahren bei Bedarf anderen Behörden (wie etwa dem Gerichtsvollzieher) oder Gerichten übermittelt.

89 Dass der Beitragsservice ein Konto anlegt bzw. die Beitragsnummer vergibt, ohne dass die betroffene Person dies erfährt, ist gesetzlich ausgeschlossen. Nach § 11 Abs. 7 S. 3 RBStV erhält jede neu angemeldete Person vom Beitragsservice eine schriftliche Anmeldebestätigung. Diese umfasst auch die Angabe der Beitragsnummer. Zwar ist nicht völlig auszuschließen, dass ein solches Schreiben abhandenkommt oder die betroffene Person es versehentlich vernichtet. Aber abgesehen davon, dass dies in datenschutzrechtlicher Hinsicht irrelevant und jedenfalls nicht dem Beitragsservice zur Last zu legen ist, hat die betroffene Person in solchen Fällen die Möglichkeit, im Wege des Auskunftsanspruchs nach Art. 15 Abs. 1 DSGVO ihre Beitragsnummer in Erfahrung zu bringen, wenn sie sich – insbesondere durch Angabe ihres vollständigen Namens mit Geburtsdatum und Adressdaten – hinreichend eindeutig identifiziert.

90 In einigen Fällen sah es eine betroffene Person umgekehrt als Verstoß gegen ihr obliegende datenschutzrechtliche Verpflichtungen an, dem Beitragsservice auf dessen Verlangen die Beitragsnummer einer anderen Person zu nennen. Anlass sind beispielsweise Anträge auf Befreiung von der Beitragspflicht unter Berufung auf Tatsachen, die in der anderen Person begründet sind. Dies betrifft etwa den Fall einer Wohngemeinschaft zwischen der antragstellenden und einer weiteren – beitragspflichtigen – Person, oder das Verhältnis zwischen dem gesetzlichen Betreuer der Bewohnerin einer Seniorenwohngemeinschaft und deren Mitbewohnerin. Im Kern geht es dabei primär jeweils um das Verständnis beitragsrechtlicher Vorschriften und nur mittelbar um deren datenschutzrechtliche Implikati-

onen. Denn aus den Vorschriften des RBStV geht hervor, dass mehrere Personen, die sich auf einen einheitlichen Beitragssachverhalt berufen, quasi als Gesamthandsgemeinschaft zu betrachten und deshalb wechselseitig im Verhältnis zueinander bzw. gegenüber dem Beitragsservice zur Information und Mitwirkung verpflichtet sind. Demzufolge muss sich der Beitragsservice in solchen Fällen nicht etwa auf anderweitige Recherche- oder Erkenntnisquellen verweisen lassen, zumal dahingehende Aktivitäten ihrerseits eine gesetzliche Grundlage voraussetzen und womöglich datenschutzrechtlich zusätzliche Fragen aufwerfen würden. Auch würde dies das Aufklärungsrisiko in Bezug auf das Bestehen der Beitragspflicht entgegen der Wertung des § 9 Abs. 1 RBStV vom Beitragspflichtigen auf den Beitragsservice verlagern und dort den Verwaltungsaufwand beträchtlich erhöhen.

91 Nach alledem bestehen aus datenschutzrechtlicher Sicht keine Bedenken gegen die Forderung des Beitragsservices, vom Betroffenen die Beitragsnummer der Person zu erfahren, die die von ihr mitbewohnte Wohnung angemeldet hat. Das mit einer fehlenden Angabe dieses Datums verbundene Risiko, selbst zur Zahlung des Rundfunkbeitrags herangezogen zu werden, liegt nach den gesetzlichen Vorschriften beim Betroffenen. Dies ergibt sich unmittelbar aus § 8 Abs. 5 RBStV für den Fall der Abmeldung. Daher ist das andere Mitglied des betreffenden Haushalts mittelbar verpflichtet, der antragstellenden Person ihre Beitragsnummer mitzuteilen – bzw. ist die antragstellende Person in datenschutzrechtlicher Hinsicht zur Weitergabe des personenbezogenen Datums der dritten Person an den Beitragsservice berechtigt - und damit dem Beitragsservice die vollständige Prüfung des für die Befreiung geltend gemachten Sachverhalts zu ermöglichen.

e Einsatz von Videokonferenzsystemen

92 Eine der markantesten Auswirkungen der Corona-Epidemie besteht darin, dass ein erheblicher Anteil der Beschäftigten berufliche Arbeiten von zuhause aus erledigen muss – aber dank rasch geschaffener technischer Infrastrukturen auch kann. Nachdem das sogenannte „Home-Office“ in Deutschland traditionell (arbeitgeberseitig) auf größte Vorbehalte gestoßen und kaum zugelassen bzw. umgesetzt war, hatte die restriktionsbedingte Notlage insoweit disruptive Kraft. Alles spricht dafür, dass sich die Arbeitsbedingungen in Deutschland dadurch strukturell verändern. Voraussichtlich ist deshalb dauerhaft mit einem deutlichen größeren Anteil von Heimarbeit auch bei den Rundfunkanstalten und ihren Beteiligungsunternehmen zu rechnen.

93 Diese Entwicklung führt unter anderem dazu, dass Arbeitsbesprechungen, Sitzungen, Versammlungen und Konferenzen häufiger als bislang gewohnt auf elektronischem Weg durchgeführt werden. Dafür können die Verantwortlichen auf zahlreiche Videokonferenzsysteme zurückgreifen, die webbasiert und deshalb relativ einfach einzusetzen sind, sich allerdings außer durch die Kosten und Technik auch in der Funktionalität und im Komfort voneinander unterscheiden. Vor allem aber gehen diese Systeme durchaus unterschiedlich mit den personenbezogenen Daten jener um, die die Technik nutzen. Der Verantwortliche muss daher das System, für dessen Einsatz er sich entscheidet, gerade auch in datenschutzrechtlicher Hinsicht umfassend prüfen und dafür sorgen, dass es die Anforderungen der DSGVO in vollem Umfang erfüllt. Dies stößt vor allem bei den – auch hier – besonders erfolgreichen Plattformen US-amerikanischer Anbieter wie vor allem Zoom oder Microsoft

Teams auf große Schwierigkeiten und erfordert entsprechenden Nachdruck, insbesondere soweit es um die Datenübermittlung in die USA geht.

94 In der Anfangszeit der Pandemie bestand eine besondere Schwierigkeit für die Verantwortlichen darin, sehr schnell geeignete technische Plattformen zur Verfügung stellen zu müssen, um den Betrieb nicht stärker als unbedingt nötig zu gefährden – gerade auch angesichts des in dieser Zeit überragenden Berichterstattungsinteresses. Zugleich war mithilfe wirksamer technischer und organisatorischer Maßnahmen ein umfassender Schutz der personenbezogenen Daten der Nutzer dieser Plattformen zu gewährleisten, denn Datenschutz hat im doppelten Wortsinne virenresistent zu sein. Um die Verantwortlichen (und die internen Datenschutzbeauftragten) insoweit zu unterstützen, habe ich die wichtigsten dabei zu berücksichtigenden Punkte in einer Orientierungshilfe[31] zusammengefasst, die auch über die Infothek meiner Website abrufbar ist.

f Nutzung von „Social Media“

95 Erneut haben mich die datenschutzrechtlichen Implikationen der sogenannten „Sozialen Netzwerke“ beschäftigt. Angesichts der zunehmenden Zahl dieser Plattformen werden die damit verbundenen Fragen immer dringlicher.

96 So stellt sich unter anderem die Frage, welche Konsequenzen sich aus der höchstrichterlichen Rechtsprechung zur datenschutzrechtlichen Einordnung der Aktivitäten von **Facebook** (dazu TB 2019, Rn. 50 ff., 68 f.) für die Rundfunkanstalten ergibt, die diese Plattform – neben etlichen anderen – als Verbreitungsweg für ihre Angebote nutzen. Jeder Besuch der dafür eingerichteten sogenannten „Fanpages“ führt zur Verarbeitung personenbezogener Daten der jeweiligen Nutzer, für die Facebook und die Rundfunkanstalt grundsätzlich gemeinsam verantwortlich sind. Beide benötigen deshalb für die ihnen zuzurechnende Datenverarbeitung jeweils eine eigene Rechtsgrundlage. Zudem fordert Art. 26 DSGVO in solchen Fällen eine Vereinbarung zwischen den beiden Verantwortlichen, die klarstellt, wie sie ihre wechselseitigen datenschutzrechtlichen Pflichten erfüllen.

97 Darüber hinaus ist seit dem Urteil des EuGH vom 16. Juli 2020 (Schrems II, oben Rn. 26 f.) klar, dass – auch – die mit der Nutzung von Facebook verbundene Datenübermittlung in die USA nur dann rechtmäßig ist, wenn die Vertragsparteien geeignete Garantien und Maßnahmen vereinbaren, die ein der DSGVO vergleichbares Schutzniveau garantieren; auf das Privacy Shield kann eine solche Datenübermittlung jedenfalls nicht mehr gestützt werden. Und schließlich ist zu berücksichtigen, dass sich nach der Rechtsprechung des Bundesverwaltungsgerichts (s. dazu TB 2019, Rn. 69) aus der gemeinsamen Verantwortlichkeit das Recht ebenso wie gegebenenfalls die Pflicht der Datenschutzaufsichtsbehörden ergibt, diese aus der DSGVO folgenden Anforderungen gegen den Betreiber der Fanpage (anstatt gegenüber Facebook) durchzusetzen, wenn sich dies als tatsächlich und rechtlich effektiver Weg erweist, schwerwiegende datenschutzrechtliche Mängel abzustellen.

[31] https://www.rundfunkdatenschutz.de/infothek/orientierungshilfe-202009.file.html/Orientierungshilfe%20202009.pdf

98 Die Rundfunkanstalten berufen sich für die Einrichtung von Facebook-Fanpages auf ihren Programmauftrag. Ihre dort verbreiteten Programminhalte bzw. die entsprechenden personenbezogenen Daten unterliegen in diesem Fall dem sogenannten Medienprivileg (§§ 12, 23 MStV). Sie selbst erheben und verarbeiten keine Daten der Nutzer ihrer über Facebook ausgespielten Inhalte. Allerdings lösen sie durch ihre Fanpage die Verarbeitung dieser Daten durch Facebook mit aus. Dafür benötigen sie deshalb (nach den oben genannten Grundsätzen der gemeinsamen Verantwortung) grundsätzlich eine eigene Rechtsgrundlage.

99 Hier ist zu unterscheiden: Soweit es sich um die Daten bereits bei Facebook registrierter Nutzer handelt, wirkt deren mit der Registrierung abgegebene Einwilligung grundsätzlich auch zugunsten der Rundfunkanstalt. Eine solche fehlt jedoch für jene Personen, die die von der Rundfunkanstalt auf einer Fanpage ausgespielten Inhalte nutzen, sich aber – im Einzelfall auch ganz bewusst – nicht bei Facebook registriert haben. Daher müssen die Rundfunkanstalten begründen, auf welche Rechtsgrundlage sie diese (von ihnen mit veranlasste) Datenverarbeitung durch Facebook stützen. Wenn sie für die Wahrnehmung ihres Funktionsauftrags erforderlich wäre, weil die Rundfunkanstalten ohne eine Verbreitung ihrer jeweiligen Programminhalte über Facebook (bzw. ohne Präsenz auf einer Facebook-Fanpage) publizistisch nicht mehr wettbewerbsfähig sind, käme dafür möglicherweise Art. 6 Abs. 1 lit. e) DSGVO in Betracht. Dann müsste die damit einhergehende Datenverarbeitung durch Facebook gleichsam die unvermeidbare Konsequenz eines aus rundfunkrechtlichen Gründen gebotenen Verhaltens sein. Alternativ kommt ansonsten – außer der expliziten Einwilligung aller Nutzer mit der Datenverarbeitung – als Rechtsgrundlage nur Art. 6 Abs. 1 lit. f) DSGVO in Betracht. Danach muss die Datenverarbeitung durch Facebook erforderlich sein, um berechtigte Interessen der Rundfunkanstalten zu wahren, und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen – insbesondere nicht bei Facebook registrierten - Personen dürfen nicht überwiegen.

100 Nach meiner Auffassung zwingt die DSGVO die Rundfunkanstalten jedenfalls dazu, sorgfältig zu begründen und die Nutzer darüber zu informieren, warum sie sich zur Erfüllung ihres Programmauftrags veranlasst sehen, Facebook-Fanpages einzurichten 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 GRCh, die DSGVO und das GG geschützt sind. Zudem haben die Rundfunkanstalten auf den Abschluss einer Vereinbarung mit Facebook hinzuwirken, die den Anforderungen von Art. 26 DSGVO genügt und die in die USA 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. Sinnvollerweise sollte sich die RDSK dazu auf einheitliche Handlungsvorgaben verständigen. Die von mir dazu angestoßene Diskussion ist noch nicht abgeschlossen.

101 Entsprechende Maßstäbe gelten selbstverständlich auch für die Nutzung anderer Netzwerke wie insbesondere das – ebenfalls zum Facebook-Konzern gehörende – Messenger System **WhatsApp**, eine Audio-Talkplattform wie „Clubhouse“ oder gar Angebote, die sich zudem noch explizit an Kinder und Jugendliche richten wie TikTok oder Instagram. Die datenschutzrechtliche Bewertung hängt dabei stets auch davon ab, ob und wie die Rund-

funkanstalt die Plattform selbst nutzt, in ihr Onlineangebot einbindet oder beispielsweise in einem ihrer Programme nur zur Nutzung eines solchen Dienstes für die Kommunikation mit der Redaktion aufruft (s. zu dieser Differenzierung bereits TB 2019, Rn. 171 ff.).

102 Erneut hat der letztgenannte Sachverhalt Nutzer öffentlich-rechtlicher Angebote im Jahr 2020 wiederholt dazu veranlasst, sich bei mir zu beschweren. Hier stellen sich allerdings weniger datenschutzrechtliche als vielmehr programmliche, ggf. auch rundfunkrechtliche Fragen. Denn selbst dort, wo eine Redaktion als Kommunikationsweg in solchen Fällen nur eine einzige dieser Plattformen anbietet, und dies – ausgerechnet – der am weitesten verbreitete, aber ähnlich wie Facebook datenschutzrechtlich problematische Dienst WhatsApp sein sollte, kann sich die Redaktion im Zweifel darauf zurückziehen, dass es letztlich jedem Nutzer freistehe, ob er diesen Kommunikationsweg nutzen wolle. Im datenschutzrechtlichen Sinne trägt die Rundfunkanstalt insoweit dann tatsächlich keine Verantwortung für die Nutzung des Dienstes bzw. die mit ihm verbundene Datenverarbeitung. Ob dies mit der besonderen Fürsorge vereinbar ist, die der dem Gemeinwohl verpflichtete öffentlich-rechtliche Rundfunk nach meinem Verständnis insoweit in Bezug auf die persönlichen Belange seines Publikums wahrnehmen sollte, steht auf einem anderen Blatt. Im Kern handelt es sich dabei um eine Frage der Programmgestaltung und -verantwortung, die infolge der Vorschriften zum sogenannten „Medienprivileg" (§§ 12, 23 MStV) nicht der Datenschutzaufsicht, sondern lediglich der in rechtlicher Hinsicht sehr begrenzten internen Programmkontrolle (letztlich durch den Rundfunkrat) unterliegt. Daher verweise ich in solchen Fällen die Beschwerdeführer durchweg an die jeweilige Rundfunkanstalt.

103 Für die redaktionsinterne Betreuung und Überwachung der Kommunikation über bzw. mithilfe solcher Plattformen können die Rundfunkanstalten auf sogenannte „**Community Management-Systeme**" zurückgreifen. Der Einsatz einer solchen Software bzw. die mit ihr verbundene Verarbeitung personenbezogener Daten der an der jeweiligen Kommunikation Beteiligten dient dem Funktionsauftrag der Rundfunkanstalten und lässt sich daher – ebenso wie die Nutzung des „Sozialen Netzwerks" als solchem – auf Art. 6 Abs. 1 lit. e) bzw. f) stützen. Die Software selbst dient der Verarbeitung personenbezogener Daten zu journalistischen Zwecken. Welchen Stellenwert sie für die redaktionelle Arbeit tatsächlich hat, ist datenschutzrechtlich unerheblich.

g Verarbeitung von Nutzungsdaten, Tracking

104 Immer wieder zeigen sich Petenten irritiert darüber, dass „ausgerechnet der öffentlich-rechtliche Rundfunk" ihre Nutzungsdaten mithilfe von Cookies ohne ihre Kenntnis bzw. Einwilligung auswerte – erst recht, wenn und soweit es dabei um Angebote geht, die sich an Kinder und Jugendliche richten bzw. (wie Phoenix oder 3sat) dem Kernbereich des öffentlich-rechtlichen Angebotsspektrums zuzurechnen sind. Dies war auch im Jahr 2020 ein häufig genannter Grund dafür, sich an mich zu wenden. Dass die Rundfunkanstalten allerdings grundsätzlich berechtigt sind, die Akzeptanz ihrer Onlineangebote auf der Basis anonymisierter statistischer Datenbestände im Sinne ihres Funktionsauftrags und damit zu publizistischen Zwecken zu überprüfen, habe ich bereits im TB 2019 (dort. Rn. 182 ff.) ausführlich erläutert. In ihrer konkreten Ausgestaltung unterscheidet sich diese Praxis signifi-

kant vom Tracking auf den Websites privatwirtschaftlicher Medienanbieter[32], und zwar sowohl von der Zielsetzung wie auch vom Umfang her.

105 Daher führte keine der bei mir eingegangenen Eingaben zur Feststellung eines Datenschutzverstoßes; wohl aber habe ich in allen Fällen die Rechtslage ausführlich erläutert und die Betroffenen außerdem auf die Möglichkeit verwiesen, der Nutzungsmessung zu widersprechen („Opt-Out"). Sie bieten alle Rundfunkanstalten an. Der in einem Beschwerdeverfahren gegen das ZDF erhobene Vorwurf, diese Opt-Out-Option bzw. deren grafische Gestaltung sei missverständlich, war nach meiner Beurteilung gemessen am Eindruck eines durchschnittlichen Nutzers nicht begründet.

106 Unabhängig davon war nach dem Urteil des BGH vom 28. Mai 2020 – I ZR 7/16 (oben Rn. 33 f.) auch noch einmal die für die Zulässigkeit des **Einsatzes von Cookies zur Nutzungsmessung** bislang ins Feld geführte Begründung kritisch zu überprüfen. Denn im Gegensatz zu vielen Fachleuten und den meisten Datenschutzaufsichtsbehörden – mich eingeschlossen – entnahm der BGH der Vorschrift des § 15 Abs. 3 TMG das Erfordernis einer Einwilligung auch für die dort genannten, nach dem Willen des Gesetzgebers an und für sich zu privilegierenden Zwecke. Letztlich konnte aber offenbleiben, ob sich diese Interpretation auf den Einsatz von Cookies durch die Rundfunkanstalten auswirkt. Denn sie verarbeiten für ihre publizistischen Zwecke ausschließlich anonymisierte Datenbestände, die keinerlei nutzerbezogene, sondern lediglich eine auf das jeweilige redaktionelle Angebot insgesamt bezogene Auswertung ermöglichen. Für diese Konstellation ist die Vorschrift des § 15 Abs. 3 TMG nicht einschlägig. Nach ihrem Sinn und Zweck sowie ihrem systematischen Zusammenhang soll die Vorschrift personalisierbare, das heißt auf einzelne Nutzer beziehbare Datenverarbeitungsvorgänge legitimieren, die personalisierbare Erkenntnisse und damit im Ergebnis ein Nutzerprofil ermöglichen. Ein solches entsteht, wenn verschiedene Einzeldaten wie z.B. die IP-Adresse sowie Zeitpunkt und Dauer einer bestimmten Dienstenutzung mit weiteren Daten zusammengeführt werden und auf diese Weise eine neue, eigenständige und über die Einzeldaten deutlich aussagekräftigere Information über den einzelnen Nutzer ermöglichen, die einem klassischen „Persönlichkeitsprofil" vergleichbar ist. Bei einer anonymisierten statistischen Auswertung geht es dem Diensteanbieter hingegen nicht um das Verhalten bzw. die Interessen einzelner Nutzer, sondern um die Resonanz auf sein Angebot in der Nutzergruppe insgesamt. Die RDSK hat im September 2020 ein in diesem Sinne aktualisiertes Positionspapier[33] verabschiedet.

107 Zunehmend stößt die bisherige Form der Nutzungsmessung im übrigen auf Hindernisse, weil bestimmte Browser oder andere Instrumente sogenannte Third-Party-Cookies generell blockieren oder aber die für die Nutzungsmessung eingesetzten Zählpixel verändern oder blockieren. Einige von den Rundfunkanstalten eingesetzte Auftragsverarbeiter haben für diesen Fall jedoch technische Lösungen entwickelt, die die Nutzungsmessung dennoch erlauben. Diese Instrumente dürfen die Rundfunkanstalten nach Auffassung der RDSK

[32] Den Einsatz von Tracking-Technologien bei den zwölf reichweitenstärksten privatwirtschaftlichen redaktionellen Online-Medien prüfen seit Sommer 2020 in einer konzertierten Aktion mehrere Landesdatenschutzbehörden, siehe dazu etwa TB 2020 des BfDI Baden-Württemberg S. 57 f.

[33] https://www.rundfunkdatenschutz.de/infothek/empfehlung-rdsk-cookies.file.html/Cookie%20Empfehlungen%20RDSK%20202009%20fin.pdf

ebenfalls einsetzen, soweit sie ihrerseits datenschutzkonform ausgestaltet sind und die Datenschutzerklärung dies ausreichend erläutert.

108 Deutlich problematischer ist der Einsatz von **Google Analytics**. Die Anwendung ermöglicht es unter anderem, die Herkunft des Besuchers einer Website und die Verweildauer auf einzelnen Seiten sowie über das Erfassen des folgenden Nutzungsverhaltens mittelbar den Erfolg von Werbekampagnen zu messen. Wenn es sich beim Websitebesucher um eine Person handelt, die einen anmeldepflichtigen Google-Dienst verwendet, ist es möglich, ihr dieses Nutzungsverhalten zuzuordnen. Die Anwendung gehört zu den am weitesten verbreiteten Trackingtools. Die staatlichen Datenschutzaufsichtsbehörden haben im Mai 2020 Hinweise zu dessen Einsatz im nicht-öffentlichen Bereich veröffentlicht[34]. Seither hat sich die Rechtslage allerdings in datenschutzrechtlicher Hinsicht insofern noch einmal verändert, als nach dem Urteil des EuGH in Sachen Schrems II jede Übermittlung personenbezogener Daten in die USA ohne ausdrückliche Vereinbarung wirksamer organisatorischer und technischer Maßnahmen, die ein der DSGVO vergleichbares Schutzniveau garantieren, unzulässig ist (oben Rn. 26 f.). Im Rahmen des nach Art. 26 DSGVO mit Google abzuschließenden Vertrags über die gemeinsame Verantwortung für die mit dem Einsatz des Trackingtools verbundene Datenverarbeitung muss der Anwender ansonsten jede Datenübermittlung in die USA (oder einen anderen Drittstaat) vollständig ausschließen und in der Lage sein, die Wirksamkeit dieses Ausschlusses gegebenenfalls auch zu überprüfen.

109 Ich selbst konnte und musste mich mit dieser Anwendung noch nicht abschließend befassen. Auf eine mir zugegangene allgemeine Anfrage eines Nutzers hin hat mir jedoch der Bayerische Rundfunk bestätigt, dass er sie seit einiger Zeit einsetzt, um die publizistische Wirksamkeit seines Angebots (BR24 und Mediathek) evaluieren und seine Gestaltung optimieren zu können. Allerdings erhebe der BR dabei keinerlei demographische Daten, und die IP-Adresse jedes Nutzers werde unmittelbar nach Erhebung im Regelfall noch in Deutschland, jedenfalls aber im Geltungsbereich der DSGVO anonymisiert. Zudem biete Google seit August 2020 die Möglichkeit, die IP-Adresse auf dem Google Tag Manager Server im BR und damit noch zu einem Zeitpunkt zu anonymisieren, zu dem Google selbst noch gar nicht auf die Daten zugreifen könne. Mit Blick auf die große Bedeutung, die der BR einer nutzerfreundlichen Präsentation und Auffindbarkeit seines Angebots für dessen publizistischen Erfolg beimisst, sieht er den Einsatz dieses Trackingtools deshalb auch ohne Einwilligung seiner Nutzer nach Art. 6 Abs. 1 lit. f) DSGVO als rechtmäßig an.

110 Eine weitere Beschwerde bezog sich darauf, dass der Bayerische Rundfunk im Zuge der Corona-Berichterstattung auf seiner Website die IP-Adresse sowie weitere Metadaten jener Nutzer, die eine sogenannte „interaktive Landkarte" anklickten, an den Anbieter einer Software übermittelte, die landkreisbezogen bestimmte statistische Angaben zur Ausbreitung der Pandemie auswertete und anzeigte. Da der vom BR dazu beauftragte Dienstleister das Angebot datenschutzrechtlich selbst und nicht als Auftragsverarbeiter des BR verantwortete, hatte der BR auf seiner Website die sogenannten Zwei-Klick-Lösung vorgesehen. Danach konnte sich jeder Nutzer in der Datenschutzerklärung des BR, der ihm den Zugang zur Anwendung des Drittanbieters ermöglichte, über die näheren Umstände der

[34] https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf

Verarbeitung informieren und ihr zustimmen oder widersprechen. Die Datenschutzerklärung erläuterte verständlich alle erforderlichen Angaben und erfüllte daher die Anforderungen der Artt. 12 und 13 DSGVO. Die IP-Adresse des Nutzers, der sich auf ihrer Grundlage für die Anzeige der „interaktiven Landkarte" entschied, wurde also nur nach dessen wirksam erteilter Einwilligung an den Drittanbieter übertragen. Dieser speicherte diese Daten nicht, sondern anonymisierte sie und generierte daraus eine anonymisierte Nutzungsstatistik. Der BR wiederum erhielt vom Drittanbieter nur die Gesamtzahl der Diagrammansichten der letzten 30 Tage. Insgesamt war dieses Verfahren nicht zu beanstanden.

111 Die vielen Eingaben rund um die Nutzungsmessung lassen 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. Der Verantwortliche hat insoweit zwar einen Formulierungs- und Gestaltungsspielraum, den er nur dann überschreitet, wenn er den mit den genannten Vorschriften verfolgten Schutzzweck erkennbar verfehlt. Der öffentlich-rechtliche Rundfunk sollte sich insoweit aber nach meiner Auffassung an einem optimalen Standard orientieren (s. in Bezug auf das Einwilligungsmanagement bereits oben Rn. 46).

h Personalisierungsfunktionen

112 Wie im Vorjahr lösten die Personalisierungsfunktionen der ZDF-Mediathek vielfach Irritationen aus. Der überproportional hohe Anteil von Eingaben dazu ist ein Indiz für die besondere Sensibilität in Bezug auf die datenschutzkonforme Ausgestaltung der Online-Angebote des öffentlich-rechtlichen Rundfunks. Es verwundert wenig, dass bei etlichen Nutzern vor allem die Abfrage der Personalausweisnummer auf Vorbehalte stößt. Und zwar obwohl das ZDF in seiner Datenschutzerklärung durchaus verständlich und transparent erläutert, dass es die Daten nur dazu benötigt, um die Altersangabe einmalig zu verifizieren, und dass es sie weder anderweitig verarbeitet noch dauerhaft speichert.

113 In der Regel beruhen die Beschwerden auf Missverständnissen in Bezug auf den Sinn und Zweck sowie den Umfang der damit verbundenen Datenverarbeitung. Aus den bereits in meinem TB 2019 (Rn. 188 ff.) geschilderten Gründen ist die vom ZDF veranlasste Verarbeitung personenbezogener Daten bei der Einrichtung eines personalisierten Accounts für die ZDF-Mediathek datenschutzkonform. Insbesondere sind die Nutzer nicht etwa infolge eines „klaren Ungleichgewichts" im Sinne des Erwägungsgrunds 43 DSGVO zu ihrer Einwilligung gezwungen. Weder beherrscht das ZDF den Markt des Online-Streamings oder agiert insoweit gar als Behörde, noch hat das Interesse Erwachsener, jugendschutzrelevante Sendungen auch jenseits der für das lineare Fernsehprogramm geltenden gesetzlichen Sendezeitbeschränkungen anschauen zu können, ein solches Gewicht, das es nahelegen oder gar erfordern würde, entsprechende Angebote in einer Mediathek grundsätzlich frei zugänglich zu machen und nur für die betroffene Altersgruppe besonderen Anforderungen zu unterwerfen.

i Datenschutz und Datenschutzaufsicht im journalistischen Bereich

114 Anfragen und Beschwerden unterschiedlichster Art haben mich zu Themen mit unmittelbarem oder mittelbarem Programmbezug erreicht. Grundsätzlich hat die Verarbeitung personenbezogener Daten zu journalistischen Zwecken – zurecht – datenschutzrechtlichen Vorgaben nicht zu entsprechen. Daher wird sie im wesentlichen auch weder durch den Internen Datenschutzbeauftragten überwacht noch unterliegt sie der Kontrolle durch die Datenschutzaufsicht (s. TB 2019, Rn. 8 ff.). Demzufolge habe ich die Petenten wegen der von ihnen behaupteten Persönlichkeitsrechtsverletzungen weit überwiegend an die jeweils verantwortliche Rundfunkanstalt verwiesen.

115 Teilweise ging es allerdings um grundsätzlichere Fragen des Datenschutzes im redaktionellen Bereich. Besonders galt das für zwei – voneinander unabhängige – Programmvorhaben des BR im Frühjahr 2020 („Wem gehört die Stadt?“) und des SR im Herbst 2020 („Wem gehört das Saarland?“). Deren Ziel war es, die Entwicklung der Miet- und Eigentumsverhältnisse im jeweiligen Sendegebiet zu beleuchten. In beiden Fällen hatten sich die Sender für die Recherche und Aufbereitung der Daten mit der gemeinnützigen Journalistenvereinigung Correctiv gGmbH zusammengetan. Eine weitere Besonderheit bestand darin, dass die Sender das Publikum in ihrem Sendegebiet dazu aufriefen, ihnen im Sinne einer „**Bürgerrecherche**“ auf einem speziell für diesen Zweck eingerichteten Portal auf ihrer Website (oder auf anderem Weg) alle ihnen verfügbaren Daten und Dokumente über das für sie jeweils maßgebliche Immobilien-Eigentums- oder Mietverhältnis zuzusenden. Verbunden war dies mit der Zusicherung, diese Daten ausschließlich für die angekündigte Berichterstattung zu diesem Thema zu verwenden und auch im übrigen alle persönlichkeits- und datenschutzrechtlichen Anforderungen strikt einzuhalten.

116 Zahlreiche dazu bei mir – teilweise zuvor bei den staatlichen Datenschutzbehörden - eingegangene Beschwerden veranlassten mich, den Sachverhalt näher aufzuklären und in datenschutzrechtlicher Hinsicht zu bewerten. Vielfach wurde beanstandet, es handele sich um eine schon grundsätzlich, aber erst recht vom Umfang her unzulässige Vorratsdatenspeicherung. Sie betreffe zudem vertrauliche Daten privater Dritter (etwa der Wohnungs-Vermieter oder -Eigentümer), die ohne deren Einwilligung den Sendern gar nicht zur Verfügung gestellt werden dürften. Insoweit könne auch das „Medienprivileg“ nicht einschlägig sein, denn darauf könnten sich private Dritte nicht berufen, geschweige denn damit den Bruch des Vertragsgeheimnisses rechtfertigen. Nicht einmal die in solchen Angelegenheiten zuständigen Behörden seien befugt, ein derart umfassendes Wohn- oder Eigentums-Register anzulegen. Darüber hinaus diene das Projekt offenbar nur einer Kampagne gegen Wohnungs-Vermieter und -eigentümer und verletze daher auch noch die für die Rundfunkanstalt maßgeblichen Programmgrundsätze.

117 Im Ergebnis waren diese Beschwerden datenschutzrechtlich durchweg unbegründet. Dass sich gerade der öffentlich-rechtliche Rundfunk mit einem nach allgemeiner Auffassung gesellschaftlich bedeutsamen Thema wie der Wohnsituation in Teilen seines Sendegebiets befassen möchte, ist allein seine programmliche Entscheidung, die ich nicht zu beurteilen habe. Das Ziel der Recherche (bzw. des Aufrufs), den für die Berichterstattung maßgeblichen Sachverhalt möglichst umfassend aufzuklären, um ihn auf dieser Basis transparent darstellen und bewerten sowie der Bevölkerung eine fundierte Meinungsbildung ermögli-

chen zu können, ist Teil der journalistischen Sorgfaltspflicht. Diese gehört zu den Kernaufgaben der Rundfunkanstalt, wie sie etwa aus § 10 MStV hervorgehen. Darüber, wie sie ihrer journalistischen Sorgfaltspflicht genügt, insbesondere welche Mittel sie dazu einsetzt, entscheidet ebenfalls ausschließlich die Rundfunkanstalt. Ob die konkrete Ausgestaltung gegen Programmgrundsätze verstößt, hat letztlich allein das für Programmfragen zuständige Organ (Rundfunk-/Fernseh-/Hörfunkrat) zu überprüfen.

118 Soweit die Rundfunkanstalt für ihre Berichterstattung personenbezogene Daten verarbeitet (insbesondere erhebt und speichert), benötigt sie dafür weder die Einwilligung der jeweils betroffenen Personen, noch muss sie sich auf einen der sonstigen Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO stützen können. Dies ergibt sich aus den §§ 12 bzw. 23 Abs. 1 S. 4 MStV, die die Verarbeitung personenbezogener Daten zu journalistischen Zwecken ausdrücklich vom Geltungsbereich dieser und zahlreicher weiterer Vorschriften der DSGVO ausnehmen; eine entsprechende Regelung enthalten die für die jeweilige Rundfunkanstalt maßgeblichen Landesgesetze bzw. -staatsverträge.

119 Diese Grundsätze gelten auch dann, wenn eine Rundfunkanstalt – wie hier - mit Dritten zusammenarbeitet. Denn ohne Zweifel diente die mit der Kooperation einhergehende Verarbeitung personenbezogener Daten journalistischen Zwecken. Im Innenverhältnis hatten die Partner die Aufgaben aufgeteilt: vereinfacht gesagt hatte es die Correctiv gGmbH übernommen, die Daten zu sammeln und aufzubereiten, während die redaktionelle Bearbeitung und Veröffentlichung in der Verantwortung der Rundfunkanstalt lag.

120 Auch der Einwand, das „Medienprivileg“ könne allenfalls die Medien berechtigten, personenbezogene Daten ohne Einwilligung der Betroffenen zu erheben, nicht aber Dritte, solche Daten weiterzugeben, ist nur vordergründig plausibel. Denn nach Sinn und Zweck der vermeintlichen „Privilegierung“ kann es nicht darauf ankommen, ob die Rundfunkanstalt die Daten selbst erhebt oder ob sie ihr Dritte übermitteln. Anderenfalls bliebe von dem aus Gründen der Rundfunk- (und Presse-)freiheit gebotenen datenschutzrechtlichen Freiraum der Medien nicht viel übrig. Entscheidend ist allein die Zielsetzung der Datenweitergabe bzw. -verarbeitung: sie muss journalistischen Zwecken dienen. Dieses Kriterium ist nach der Rechtsprechung des EuGH weit auszulegen (s. TB 2019, Rn. 8, 49). Hier bestand daran schon deshalb kein Zweifel, weil beide Landesrundfunkanstalten den Anlass der „Bürgerrecherche“ bzw. ihres Aufrufs zur Datenübermittlung an sie vorab auf ihren Websites eingehend erläutert und mit der vorgesehenen Berichterstattung begründet hatten.

121 Auch auf den Umfang und den Charakter des im Zuge der Recherche entstehenden Bestands an (personenbezogenen) Daten kommt es für die datenschutzrechtliche Bewertung nicht an. Eine Recherche wird nicht deshalb datenschutzrechtlich problematisch, weil sie besonders umfassend und gründlich, also etwa darauf angelegt ist, einen möglichst umfangreichen Datenbestand zu generieren. Das ergibt sich schon daraus, dass die Frage, welche Daten in welchen Umfang für eine Berichterstattung benötigt werden, vom jeweiligen Sachverhalt abhängen, insbesondere von dessen Gegenstand, Komplexität und (rechtlicher oder gesellschaftlicher) Auswirkung. Insoweit sei beispielsweise an die deutlich umfangreicheren Datenbestände im Zuge der "Panama-Paper"-Affäre aus dem Jahr 2016, den "Cum-Ex-Skandal" aus dem Jahr 2018 oder ähnliche Berichterstattungsgegenstände aus jüngerer Zeit erinnert. Wie umfangreich und tiefgehend die Recherche bzw. der für die

Berichterstattung gewünschte oder erforderliche Datenbestand anzulegen ist, gehört daher zu den originären Entscheidungen der Rundfunkanstalt im Rahmen ihrer journalistischen Sorgfaltspflicht.

122 Es kennzeichnet eine besonders gründliche und umfassende Recherche geradezu, dass die dabei entstehenden Datenbestände deutlich umfangreicher sind als die auf ihnen beruhende Berichterstattung. Denn die Freiheit der Recherche, die durch die Rundfunkfreiheit nach Art. 5 Abs. 1 S. 2 GG umfassend gerade auch gegen datenschutzrechtlich motivierte Beschränkungen geschützt ist, bedeutet keineswegs, dass die Rundfunkanstalt mit den dabei erhobenen bzw. verarbeiteten personenbezogenen Daten nach Gutdünken verfahren dürfte. Vielmehr gehört es zu den essentiellen Aufgaben der journalistischen Sorgfaltspflicht, darüber zu entscheiden, ob und in welcher Form diese Daten anschließend veröffentlicht werden dürfen. Dabei hat die Rundfunkanstalt wie in ihrer sonstigen Berichterstattung auch stets die Persönlichkeitsrechte aller betroffenen Personen zu beachten. Darüber hinaus unterliegen die mit der Recherche bzw. Berichterstattung befassten Personen sämtlich der Verpflichtung, das Datengeheimnis zu wahren und die verarbeiteten personenbezogenen Daten angemessen zu schützen, §§ 12 Abs. 1, 23 Abs. 1 MStV. Und schließlich stehen betroffenen Personen im Falle einer rechtswidrigen Veröffentlichung außer zivil- bzw. äußerungsrechtlichen Ansprüchen unter den dort jeweils genannten Voraussetzungen die Rechte aus den §§ 12 bzw. 23 Abs. 2 und 3 MStV zu. Diese – und nur diese – Vorgaben können gegebenenfalls auch im Wege der Datenschutzaufsicht überprüft und sanktioniert werden.

123 Dass die beiden Landesrundfunkanstalten jeweils mit der Correctiv gGmbH kooperierten, warf im übrigen auch die Frage der aufsichtsrechtlichen Zuständigkeit auf. Denn die unabhängige Journalistenvereinigung hat als juristische Person ihren Sitz in Nordrhein-Westfalen und unterliegt damit grundsätzlich der Zuständigkeit der dortigen Landesdatenschutzbeauftragten. Da die „Bürgerrecherche" aber einem Programmvorhaben der beiden Landesrundfunkanstalten diente und die Verantwortung insoweit bei diesen lag, war für die aufsichtsrechtliche Bewertung, auch soweit sie sich direkt oder indirekt auf Tätigkeiten der Correctiv gGmbH bezog, ausschließlich ich zuständig.

124 Es ist damit zu rechnen, dass Projekte dieser Art als Ausprägung des **Datenjournalismus** zunehmen werden. Aufsehenerregende investigative Recherchen und Veröffentlichungen wie etwa die der „Süddeutschen Zeitung" (auch gemeinsam mit Landesrundfunkanstalten wie etwa NDR und WDR) über die „Panama Papers" legen davon Zeugnis ab. Sie sind unter anderem durch die projektbezogene oder auch auf längere Dauer angelegte Zusammenarbeit mehrerer Medienunternehmen oder journalistische Organisationen sowie die Verarbeitung enormer Datenmengen gekennzeichnet, die für die Berichterstattung ausgewertet werden.

125 Dies wirft in datenschutzrechtlicher Hinsicht einige neue Fragen auf, die eine genauere Betrachtung verdienen, denen ich aber noch nicht vertieft nachgehen konnte oder musste. Dazu gehört, inwieweit die Rundfunkanstalten die Modalitäten der Datenverarbeitung in einem solchen Kooperationsverhältnis im einzelnen vertraglich regeln sollten, und zwar sowohl im Hinblick auf die Zielsetzung als auch auf die Dauer der Datenverarbeitung. Denn die Kooperation ist im Zweifel befristet, der Datenbestand hingegen kann theoretisch dau-

erhaft gespeichert, mit unterschiedlichen Zielsetzungen ausgewertet und dabei auch mit anderen Datenbeständen zusammengeführt werden, sofern die Datenerhebung bzw. -verarbeitung nicht ausdrücklich auf das konkrete, aktuelle redaktionelle Vorhaben beschränkt wurde. Dafür ist unter anderem entscheidend, wer bis wann und zu welchen Zwecken auf den Datenbestand zugreifen kann. Unabhängig davon stellt sich angesichts der enormen Datenmengen, die solche Großprojekte generieren, mehr noch als bei sonstigen journalistischen Recherchedaten die Frage angemessener technischer und organisatorischer Maßnahmen, die die Integrität und Vertraulichkeit der Daten gewährleisten können. Dazu kann neben den gebotenen technischen Vorkehrungen und sonstigen Sicherungsmaßnahmen beispielsweise gehören, dass der Zugriff auf die Datenbanken nur bestimmten (journalistisch tätigen) Personen möglich ist und jeweils protokolliert wird.

126 Staatliche und Rundfunkdatenschutzaufsicht gleichermaßen sind potentiell auch betroffen, wenn es um **Rechercheaktivitäten in sensiblen Situationen** geht. Typische Fälle insoweit sind etwa Dreharbeiten bei Polizei- oder Feuerwehreinsätzen (s. dazu TB 2019, Rn. 200), in Kindergärten oder Schulen, im Krankenhaus, in Obdachlosenunterkünften oder bei Zwangsvollstreckungsmaßnahmen. Typischerweise gilt für alle unmittelbar programmbezogenen – journalistischen – Aktivitäten das „Medienprivileg“, und im Zweifel liegt die Zuständigkeit bei der Rundfunkdatenschutzaufsicht. Soweit es allerdings um die Bereitschaft von Behörden oder Amtsträgern geht, sich bei der Arbeit begleiten oder Aufnahmen in ihren Gebäuden zuzulassen, sind für die Klärung datenschutzrechtlicher Fragen und etwaige Empfehlungen oder Vorgaben für entsprechende Genehmigungen deren behördliche Datenschutzbeauftragte sowie die jeweilige staatliche Datenschutzaufsichtsbehörde zuständig. Daraus folgt allerdings nicht etwa, dass die staatliche Aufsicht womöglich Vorgaben zur Gestaltung oder Ausstrahlung eines entsprechenden Programmbeitrags bzw. zur Verarbeitung, insbesondere Speicherung bzw. Löschung der dabei verarbeiteten personenbezogenen Daten machen könnte. Die Entscheidung darüber liegt vielmehr weder bei der Rundfunk- noch gar bei der staatlichen Datenschutzaufsicht, sondern ausschließlich in der Verantwortung der Rundfunkanstalt. Anlässlich eines einschlägigen Vorgangs beim ZDF war der Eindruck entstanden, dass die zuständige Landesdatenschutzbehörde insoweit anderer Auffassung sei; dies hat sich jedoch nicht bestätigt.

j Beschäftigtendatenschutz

127 Mit Fragen zum Beschäftigtendatenschutz habe ich mich überwiegend nur im Rahmen von Erörterungen mit den Datenschutzbeauftragten in meinem Zuständigkeitsbereich befasst. Unter anderem habe ich auf den entsprechenden Wunsch hin zu einem Teilaspekt des anstaltsübergreifenden Projekts „(D)ein SAP“ Stellung genommen. Eine bei mir eingegangene Meldung nach Art. 33 DSGVO ging darauf zurück, dass bei der raschen Umstellung des Betriebs auf „Home-Office“ zunächst übersehen worden war, dass bei der dazu eingerichteten Rufumleitung in einigen Fällen externen Anrufern nicht die von ihnen angewählte dienstliche, sondern die Privatnummer der angerufenen Person angezeigt wurde. Angesichts der konkreten Umstände und rascher Abhilfe durch den Verantwortlichen war damit jedoch kein nennenswertes Risiko für die Rechte und Freiheit der Betroffenen verbunden und es bestand kein weiterer aufsichtsrechtlicher Handlungsbedarf. In einem anderen Fall zog eine Petentin ihre zunächst bei der staatlichen Datenschutzaufsicht eingereichte und

von dort an mich abgegebene Beschwerde zurück, sodass ich den von ihr beklagten Datenschutzverstoß nicht überprüfen musste. In einem Beteiligungsunternehmen gab es Auseinandersetzungen um die Wirksamkeit von Löschvorgaben, die allerdings zunächst mit dem Verantwortlichen und dessen Auftragsverarbeiter zu klären waren.

128 Grundsätzlich spricht das bisher geringe Anfrage- bzw. Beschwerdeaufkommen aus diesem Bereich dafür, dass der Schutz der personenbezogenen Daten aller Beschäftigten 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 Rundfunkanstalten Beschäftigten die Option, sich an die spezifische Rundfunkdatenschutzaufsicht zu wenden, noch nicht bewusst ist, nachdem über Jahrzehnte hinweg in solchen Fällen (nur) der Weg zum internen Datenschutzbeauftragten zur Verfügung stand.

4 Meldungen nach Art. 33 DSGVO

129 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[35]. Dabei ist es zunächst stets Sache des Verantwortlichen zu prüfen, ob die Voraussetzungen eines meldepflichtigen Vorgangs und der in den Fällen des Art. 34 DSGVO vorgeschriebene Benachrichtigung davon betroffener Personen vorliegen. Damit trägt er auch das Risiko eines etwaigen schuldhaften Unterlassens. Ein solches kann zu aufsichtsrechtlichen Sanktionen führen. Im Zweifel sollte der Verantwortliche daher stets die Aufsicht benachrichtigen. Daraus geht zugleich hervor, dass allein die Tatsache einer Meldung nach Art. 33 DSGVO in der Regel noch keine Rückschlüsse darauf zulässt, ob die Datenschutzverletzung auf strukturelle, organisatorische, technische oder personelle Ursachen zurückgeht und ob der Vorfall im engeren Sinne aufsichtsrechtlich relevant ist. Auf zwei mir gemeldete Sachverhalte gehe ich hier etwas näher ein.

130 Bereits im Oktober 2019 hatte mir das ZDF zwei in kurzer Zeit aufeinander folgende, mittelbar miteinander verbundene Datenschutzvorfälle gemeldet, deren aufsichtsrechtliche Prüfung und Bewertung ich erst im Januar 2020 abschließen konnte. Beide betrafen die Konfiguration des Accounts „Mein ZDF“ und damit die Personalisierungsfunktion der ZDF Mediathek. In beiden Fällen konnten registrierte Inhaber eines solchen personalisierten Zugangs nachts über einige Zeit hinweg personenbezogene Daten anderer Inhaber eines solchen Accounts einsehen. Während im ersten Fall ein Konfigurationsfehler des Software-Updates ursächlich war, führte im zweiten Fall wenig später ein Versehen bei der Installation der verbesserten Software zu demselben Problem. In beiden Fällen hatte sich das ZDF der Unterstützung externer Auftragsverarbeiter bedient, deren Aktivitäten ich deshalb ebenfalls aufsichtsrechtlich zu überprüfen und zu bewerten hatte, Art. 58 Abs. 1 DSGVO.

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

131 Das ZDF hat mir die Vorfälle fristgerecht gemeldet und nach Feststellung des Problems jeweils unverzüglich und sachgerecht reagiert. Seine Bewertung, dass das mit den beiden Vorfällen verbundene Risiko für die Rechte und Freiheiten betroffener Nutzer der ZDF Mediathek als eher gering zu bewerten und deshalb eine Benachrichtigung dieses Personenkreises gem. Art. 34 DSGVO nicht erforderlich sei, habe ich mich angeschlossen. Allerdings waren geeignete organisatorische Maßnahmen zu veranlassen, die die Wiederholung eines derartigen Vorfalls ausschließen, Art. 58 Abs. 2 lit. d) DSGVO. Über die Umsetzung dieser Maßnahmen hat mich das ZDF ordnungsgemäß informiert. Weitergehender aufsichtsrechtlicher Handlungsbedarf bestand daher nicht; gleiches galt in Bezug auf die beiden Unternehmen, die das ZDF als Auftragsverarbeiter eingesetzt hatte.

132 Ein in gewisser Hinsicht vergleichbares Problem trat bei der ARD.ZDF Medienakademie auf. Diese hatte auf ihrer von einem Dienstleister betreuten Homepage ein Online-Bewerbungsportal für den von ihr ausgelobten Förderpreis eingerichtet. Ein weiteres Unternehmen hostete den dafür erforderlichen Server. Dieses stellte Anfang Mai 2020 fest, dass über diesen Server bzw. die dort für die Medienakademie betriebene Website Spam-Mails versandt worden waren. Daraufhin sperrte der Auftragsverarbeiter unverzüglich den Zugang zum Server sowie die SMTP-Funktion und löschte die für den Versand der Spam-Mails angelegten neuen Mail-Ordner. Die Ursachen für den zugrunde liegenden Hacker-Angriff konnte die Medienakademie bzw. ihre Auftragsverarbeiter nicht aufklären. Allerdings hatten nach meinen Feststellungen die Beteiligten die Datenverarbeitung für das Bewerbungsportal über die genannte Website offenbar nicht mit der gebotenen Sorgfalt durchgeführt, insbesondere keine ausreichenden technischen und organisatorischen Vorkehrungen getroffen, um einen solchen Hacker-Angriff zu unterbinden. Immerhin ergriff die Medienakademie jedoch nach Kenntnis des Vorfalls unverzüglich adäquate Maßnahmen und zeigte diesen auch fristgerecht bei mir an. Künftig wird sie das Bewerbungsverfahren für den Förderpreis nicht mehr über ein solches Online-Portal abwickeln. Daher kann sich ein solcher Vorfall nicht wiederholen.

5 Auftragsverarbeitung

133 Außer im Bereich der Datenverarbeitung für journalistische Zwecke, für die die entsprechenden Regelungen gemäß § 12 bzw. § 23 Abs. 1 S. 4 MStV nicht gelten (s. TB 2019, Rn. 172), erstreckt sich meine Aufsichtszuständigkeit nicht nur auf die Verantwortlichen, sondern auch auf die von ihnen beauftragten Auftragsverarbeiter. Dies bedeutet, dass sich sowohl die Aufgaben nach Art. 57 als auch die Befugnisse nach Art. 58 DSGVO auf den vom Verantwortlichen eingeschalteten Auftragsverarbeiter beziehen.

134 Mit damit verbundenen Fragen hatte ich mich vor allem in den oben (Rn. 129 ff) bereits geschilderten Fällen zu befassen, in denen mir die Verantwortlichen eine Datenschutzverletzung nach Art. 33 DSGVO gemeldet hatten. Ein Petent wandte sich an mich, weil er es als datenschutzrechtlich problematisch bzw. Verstoß des WDR gegen dessen eigene Datenschutzerklärung ansah, dass ihm auf eine Frage, die er über das vom WDR angebotene Kontaktformular gestellt hatte, ein vom WDR beauftragter Dienstleister antwortete, der zudem nach Auffassung des Petenten in der Branche nicht gut beleumundet sei. Tatsächlich klärt

der WDR jedoch in seinen Datenschutzhinweisen ausdrücklich und ordnungsgemäß über den Einsatz externer Dienstleister für solche Zwecke auf und weist darauf hin, dass diese vertraglich verpflichtet sind, dabei verarbeitete personenbezogene Daten ausschließlich für den beauftragten Zweck zu nutzen. Die personenbezogenen Daten werden also in diesen Fällen nicht an Dritte übermittelt.

135 Nur im Sinne einer ersten Einschätzung hat mich außerdem beschäftigt, welche Anforderungen an die Ausgestaltung eines Auftragsverarbeitungsverhältnissen zu einem Dienstleister außerhalb des Geltungsbereichs der DSGVO zu stellen sind. Gemäß Art. 44 Abs. 1 DSGVO ist in diesen Fällen jede Übermittlung personenbezogener Daten nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in den Artt. 44 ff. DSGVO niedergelegten Bedingungen sowie die sonstigen Bestimmungen der DSGVO einhalten. Insoweit steht der Verantwortliche vor dem praktischen Problem, ein der DSGVO vergleichbares angemessenes Schutzniveau nicht nur mithilfe vertraglicher Vereinbarungen gegenüber dem Auftragsverarbeiter durchsetzen, sondern sich auch über die praktische Umsetzung vergewissern zu müssen. Dabei stellt sich unter anderem die Frage, in welcher Form derartige Nachweise zu erbringen sind, und ob bzw. inwieweit der Verantwortliche gegebenenfalls auch veranlasst sein kann, sich vor Ort von der vertrags- (und DSGVO-)konformen Umsetzung zu überzeugen.

6 Kontrollen und Prüfungen

136 Zu den Aufgaben des Rundfunkdatenschutzbeauftragten gehört es gemäß Art. 57 Abs 1 lit. a) und Art. 58 Abs. 1 lit. b) DSGVO, 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 von geplanten Audits stattfinden. Im Jahr 2019 hatte ich dazu einen Prüfplan entwickelt. Er sieht ein jährliches Audit bei einer oder mehreren Organisationen in meinem Zuständigkeitsbereich zu einem bestimmten Schwerpunktthema vor, über das ich die Verantwortlichen jeweils rechtzeitig vorher informiere. Dabei soll es nicht nur darum gehen festzustellen, inwieweit die Vorgaben der DSGVO jeweils bereits umgesetzt sind. Sondern mittelbar geht es auch darum, auf möglichst einheitliche Standards in den Rundfunkanstalten meines Zuständigkeitsbereichs hinzuwirken. Ob und wie sich dieses Vorhaben – auch angesichts der sehr begrenzten Ressourcen - tatsächlich umsetzen lässt, muss sich zeigen.

137 Im Jahr 2020 habe ich das erste Audit durchgeführt. Bewusst habe ich mich für das **Verzeichnis von Verarbeitungstätigkeiten** entschieden. Ein solches hat jeder Verantwortliche nach den Vorgaben von Art. 30 DSGVO anzulegen. Wie bei allen Anforderungen, die über die „eigentliche“ Geschäftstätigkeit (für Programm, Produktion und Verwaltung) hinaus Aufwand und Zeit in Anspruch nehmen, besteht die Gefahr, dass eine derartige Vorgabe als unnötig formalistisch und disponibel empfunden und daher gern „auf die lange Bank geschoben“ wird, weil es im Zweifel im Tagesgeschäft stets Dringlicheres zu erledigen gibt. Tatsächlich erfordert es erst einmal Mühe, ein ordnungsgemäßes Verzeichnis nach Art. 30 DSGVO zu entwickeln. Dann aber ist es ein bedeutsames Instrument, um die Einhaltung des Datenschutzes innerhalb eines Unternehmens zu gewährleisten: Es verschafft dem Verantwortlichen den Überblick über alle Prozesse und Mittel der Datenverarbeitung und ermög-

licht den Nachweis, dass er die Vorgaben der DSGVO einhält. Es gehört zu den wichtigsten Grundlagen der Beratungs- und Überwachungsfunktion des internen Datenschutzbeauftragten. Und schließlich ist es für die Aufsichtsbehörde relevant, der es gemäß Art. 30 Abs. 4 DSGVO auf Anfrage zur Verfügung zu stellen ist, um ihr im Bedarfsfall eine detailliertere Prüfung einzelner Datenverarbeitungstätigkeiten zu ermöglichen.

138 Infolge des Personalwechsels in meiner Behörde und der pandemiebedingten Komplikationen konnte ich den vorgesehenen Zeitplan zwar nicht ganz einhalten und musste mich auf strukturelle Aspekte sowie eine Stichprobenprüfung der Umsetzung in der Praxis beschränken; der damit verbundene Aufwand allerdings war immer noch beträchtlich. Immerhin aber konnte ich das Audit noch vor dem Jahresende abschließen. Die Zusammenarbeit mit den in allen fünf Fällen als Ansprechpartner für das Verfahren benannten Datenschutzbeauftragten war kooperativ. Über das Ergebnis der Prüfung habe ich die Verantwortlichen jeweils förmlich unterrichtet.

139 Das Audit diente in erster Linie einem Soll-/Istabgleich, um in Bezug auf die seit Ende Mai 2018 geltenden Vorgaben des Art. 30 DSGVO Anpassungs- und Optimierungsbedarf aufzuzeigen, nicht hingegen der Sanktionierung dabei festgestellter Defizite. Solche habe ich in unterschiedlichem Umfang in allen fünf Prüfverfahren festgestellt. Struktureller Klärungsbedarf zeigte sich in Bezug auf die Gemeinschaftseinrichtungen der Rundfunkanstalten. Insgesamt waren bzw. sind jedoch alle Verantwortlichen um ein DSGVO-konformes Verarbeitungsverzeichnis bemüht und haben das Audit insoweit auch als förderlich empfunden. Um den weiteren Bearbeitungsaufwand nicht unnötig zu erhöhen, habe ich davon abgesehen, gemäß Art. 58 Abs. 2 lit. d) DSGVO in Bezug auf einzelne festgestellte Defizite konkrete Umsetzungsmaßnahmen und -fristen anzuordnen. Stattdessen habe ich den Verantwortlichen Gelegenheit gegeben, die erforderlichen Maßnahmen unter Berücksichtigung meiner Hinweise bis Ende Mai 2021 umzusetzen, und sie gebeten, mich bis dahin über den Vollzug zu informieren.

140 Parallel zum Audit habe ich bei den meisten Beteiligungsunternehmen der Rundfunkanstalten innerhalb meines Zuständigkeitsbereichs[36] im Jahr 2020 eine **Querschnittsprüfung** durchgeführt. Ziel der mehr als 20 Abfragen war es, einen ersten Überblick darüber zu erhalten, ob und inwieweit die Anforderungen der DSGVO in den jeweiligen Unternehmen bereits umgesetzt sind. Zugleich sollte die Prüfung den Verantwortlichen signalisieren, dass sie gegebenenfalls mit konkreten Nachfragen zu rechnen haben und sich deshalb, sofern noch nicht oder nicht hinreichend geschehen, des Themas annehmen müssen. Dazu habe ich sie gebeten, einen von mir entwickelten Fragebogen auszufüllen und mir auszugsweise bestimmte Unterlagen zu überlassen. In vergleichbarer Weise sind in den beiden zurückliegenden Jahren staatliche Datenschutzaufsichtsbehörden gegenüber kleineren und mittleren Unternehmen in ihren Zuständigkeitsbereichen vorgegangen.

141 Alle von mir kontaktierten Verantwortlichen beantworteten die von mir gestellten Fragen und stellten mir die erbetenen Unterlagen zur Verfügung. Soweit im Rahmen einer derartigen kursorischen Prüfung möglich, vermittelte mir das Verfahren den Eindruck, dass die

[36] Siehe Übersicht auf meiner Website: https://www.rundfunkdatenschutz.de/ueber-uns/aufsicht-ueber-sonstige-einrichtungen-und-beteiligungsunternehme.html

Verantwortlichen die Anforderungen der DSGVO – unbeschadet von Unterschieden und Defiziten im einzelnen – im großen Ganzen kennen und sich um eine Umsetzung bemühen. Die Zusammenarbeit mit den internen Datenschutzbeauftragten oder anderweitigen Ansprechpartnern verlief sehr kooperativ und reibungslos.

7 Zahlen und Fakten 2020

142 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 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 statistische Kenndaten meiner Tätigkeit im Jahr 2020 dargestellt.

143 Im Jahr 2020 haben mich insgesamt rund 200 Zuschriften erreicht, mit denen sich außenstehende Dritte an mich gewandt haben. Berücksichtigt sind hierbei nur die durch externe Eingaben veranlassten 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 umfangreichen Prüfvorgänge, mit denen ich in anderen Zusammenhängen befasst war.

144 Die weit überwiegende Zahl der Eingaben erreicht mich per mail oder über das auf meiner Website angebotene Kontaktformular, ein kleiner Teil auf dem Postweg. Die Pandemie hat – ein wenig überraschend - nicht zu mehr Beschwerden geführt. Der zwischenzeitliche deutliche Anstieg in der zweiten Hälfte des Jahres 2019 setzte sich nicht fort; durchschnittlich haben mich monatlich etwa 16 Eingaben erreicht.

a Beschwerde

145 Mit einer Beschwerde reklamiert die betroffene Person, selbst von einer Datenschutzverletzung betroffen zu sein. Insgesamt gingen mir über 70 förmliche Beschwerden zu. Mehr als die Hälfte von ihnen betraf den Beitragsservice von ARD, ZDF und Deutschlandradio; teilweise handelte es sich dabei um Standardtexte, die einschlägige Onlineplattformen wie „Hallo Meinung“ anbieten und in denen er pauschal der Verletzung bestimmter Vorgaben der DSGVO bezichtigt wird. Fünfzehn Beschwerde richteten sich gegen den BR, sieben gegen das ZDF, vier gegen den SR, je zwei gegen den WDR und das Deutschlandradio sowie je eine gegen 3sat und Phoenix. Insgesamt sieben Beschwerden erwiesen sich als berechtigt, alle anderen habe ich nach Prüfung als unbegründet abgewiesen.

b Anzeige

146 Gelegentlich reklamiert eine Person eine vermeintliche Datenschutzverletzung, die (im Gegensatz zur Beschwerde) nicht unmittelbar sie selbst, sondern andere betrifft. Die Grenzen zur Beratungsanfrage (siehe c) sind hier fließend; außerdem betreffen derartige Eingaben

häufig (vermeintliche) Datenschutzverstöße in Sendungen der Rundfunkanstalten. In zwei Fällen ging es dabei um Verhalten einer Redaktion bzw. einer Journalistin im Umfeld der jeweiligen Sendung, aber ohne unmittelbaren Bezug zum Programm. Zu vier dieser Anzeigen habe ich ausführlich Stellung genommen.

c Beratungsanfrage

147 In einer Beratungsanfrage werden allgemeine Fragen zum Datenschutz und der Handhabung von Daten bei den Rundfunkanstalten aufgeworfen. Die Hälfte dieser insgesamt 12 Eingaben habe ich inhaltlich beantwortet und die Rechtslage erläutert; die restlichen waren aus formellen Gründen an andere Stellen zu verweisen.

d Datenschutz im Programm

148 Dass die Datenverarbeitung zu journalistischen Zwecken weder den allgemeinen Datenschutzbestimmungen noch der Datenschutzaufsicht unterliegt, ist vielfach nicht hinreichend bekannt. 2020 erreichten mich dazu mehr als 30 Eingaben sowohl von Einzelpersonen als auch von Branchen-Organisationen, von denen sich über die Hälfte auf die bereits oben (Rn. 115 ff.) behandelten „Bürgerrecherche-Projekte" von BR und SR bezogen. Zu ihnen habe ich jeweils ausführlich Stellung genommen und die Rechtslage erläutert. In den sonstigen Fällen, von denen 11 den WDR, 2 das ZDF und einer Phoenix betrafen, habe ich die Petenten in der Regel an den Verantwortlichen verwiesen und mich nur vereinzelt inhaltlich geäußert.

e Auskunftsersuchen

149 Auch meine Aufsichtsbehörde verarbeitet personenbezogene Daten. Sie ist insoweit nach meinem Verständnis 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 und nicht etwa (auch) die von den (anderen) Verantwortlichen in meinem Zuständigkeitsbereich verarbeiteten Daten. Das Gros der entsprechenden Eingaben bezog sich jedoch auf das Beitragsverhältnis oder eine der Rundfunkanstalten, die die Anspruchsteller durch mich vertreten glaubten und an die ich sie daher verwiesen habe.

150 Fünf Auskunftsbegehren gemäß Art. 15 Abs. 1 DSGVO richteten sich direkt oder inzident an mich als Aufsichtsbehörde. In keinem dieser Fälle waren bereits personenbezogene Daten zu der jeweiligen Person bei mir verarbeitet worden. Alle Auskunftsbegehren habe ich fristgerecht beantwortet.

f Sonstiges

151 Als eine der Aufsichtsbehörden für den Zentralen Beitragsservice wird der Rundfunkdatenschutzbeauftragte häufig in Bezug auf Kontenklärungen und Beschwerden bezüglich des

Rundfunkbeitrags angeschrieben. Grund 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 Beitragsservice. Dies traf auf weit mehr als 40 der bei mir eingegangenen Eingaben zu.

152 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 mehrere monatlich erreichten, äußere ich mich generell nicht inhaltlich, selbst wenn dies nach erstem Anschein mit keinem größeren Aufwand verbunden wäre. Denn ich halte es für unabdingbar, 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 aufzuzeigen.

153 Auch zahlreiche Eingaben ohne jeden oder hinreichend konkreten Datenschutzbezug haben mich erreicht. 18 von ihnen habe ich an die zuständige Stelle verwiesen.

154 Des weiteren sind bei mir einige Anfragen bzw. Auskunftsersuchen auf der Grundlage von Formularen der Website „Frag den Staat“ eingegangen. So machten zwei Antragsteller unter Berufung auf die Vorschriften des Informationsfreiheitsgesetzes (IFG), des Umweltinformationsgesetzes (UIG) sowie des Gesetzes zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (VIG) Ansprüche auf Auskunft und Information sowie Überlassung von Unterlagen zu unterschiedlichen Sachverhalten gegen mich geltend. Abgesehen davon, dass die betreffenden Bundesgesetze auf meine rundfunkspezifische Datenschutzaufsichtsbehörde gar nicht anwendbar sind, gingen die Ansprüche auch deshalb ins Leere, weil sie sich weder auf ein Umwelt- noch ein gesundheitsbezogenes Anliegen bezogen.

155 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 2020 mehrfach Gebrauch gemacht.

g Datenschutzvorfall

156 Eine Verletzung der Datenschutzvorgaben ist hier als Datenschutzvorfall bezeichnet. Ein solcher kann durch die verantwortliche Stelle selbst gemeldet werden oder aus einer durch eine Anzeige oder Beschwerde ausgelösten Untersuchung des Rundfunkdatenschutzbeauftragten hervor gehen (siehe auch oben Rn. 129 ff.).

157 2020 wurden mir 6 Datenschutzvorfälle gemeldet, für die ich unmittelbar zuständig war. Davon betrafen zwei den WDR und jeweils einer den BR, den Beitragsservice, die ARD/ZDF Medienakademie sowie – im Rahmen des mit meiner Behörde bestehenden Auftragsverarbeitungsverhältnisses – den rbb. Überwiegend hatten die Verantwortlichen dafür auf das von mir auf der Homepage zur Verfügung gestellte Meldeformular zurückgegriffen, das auf alle anzeigepflichtigen Informationen hinweist. In allen Fällen ging die Meldung innerhalb der von Art. 33 DSGVO vorgegebenen Frist bei mir ein.

h Beratung

158 Die Verantwortlichen bzw. ihre Datenschutzbeauftragten haben sich 2020 vielfach in unterschiedlicher Weise mit der Bitte um Beratung bzw. aufsichtsrechtliche Bewertung von Sachverhalten an mich gewandt. Meist ging es um Themen aus einer der Rundfunkanstalten oder dem Beitragsservice, in einem Fall um ein Beteiligungsunternehmen.

i Gerichtsverfahren

159 Im Berichtszeitraum war eine Klage gegen einen von mir erlassenen Bescheid vor dem örtlich für meine Behörde zuständigen Verwaltungsgericht Potsdam anhängig. Bislang hat sie der Kläger noch nicht begründet.