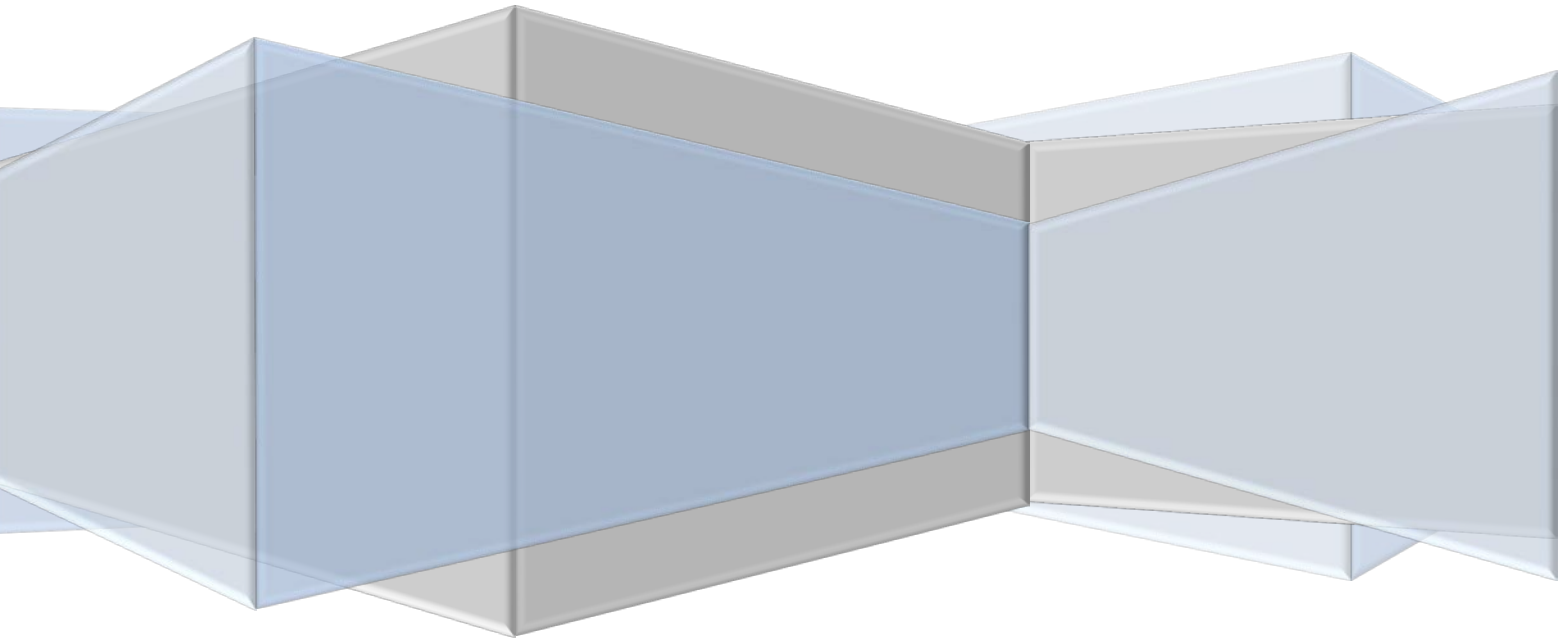
MITTELDEUTSCHER RUNDFUNK
Anstalt des öffentlichen Rechts

Tätigkeitsbericht des Rundfunkdatenschutz-beauftragten des MDR

Zeitraum 01.08.2018 bis 31.12.2019

Stephan Schwarze



Inhaltsverzeichnis

1. Einleitung

Mit dem Tätigkeitsbericht komme ich meiner Pflicht aus § 42b Abs. 4 des MDR-Staatsvertrages nach. Dies ist der erste Tätigkeitsbericht, den ich in meiner neuen Funktion als Rundfunkbeauftragter für den Datenschutz gemäß §§ 42 ff. MDR-Staatsvertrages verfasse. In meinem letzten Tätigkeitsbericht - noch in meiner Funktion als Datenschutzbeauftragter nach § 42 Abs. 1 MDR-Staatsvertrag (alt) - habe ich darauf hingewiesen, dass ich mit Wirkung zum 01.08.2018 zum Rundfunkdatenschutzbeauftragten ernannt worden bin. Aufgrund dessen und um eine Kontinuität des Berichtswesens zu gewährleisten, werde ich meinen auf das Kalenderjahr zugeschnittenen Bericht dieses Mal um die Monate August 2018 bis Dezember 2018 ausweiten, so dass dieser Bericht den Zeitraum vom 1. August 2018 bis 31. Dezember 2019 umfasst. Im nächsten Bericht (über das Jahr 2020) wird die vorgesehene jährliche Berichterstattung eingehalten.

Auch nach der neuen Rechtslage (§ 42b Abs. 2 MDR-Staatsvertrag) kann der Rundfunkdatenschutzbeauftragte förmliche Beanstandungen gegenüber der Intendantin aussprechen, sobald ein Verstoß festgestellt worden ist. Zweifellos ist es so, dass auch beim MDR die Umsetzung der Datenschutzgrundverordnung im Jahr 2018 noch nicht vollständig abgeschlossen ist und an der einen und der anderen Stelle noch nachjustiert und neu gedacht werden muss. Jedoch konnte ich keine gravierenden Datenschutzverstöße feststellen, die zu einer Beanstandung hätten führen müssen. Dies ist auch nach meinem Verständnis nur dann opportun und sinnvoll, wenn eine Behebung des Mangels und eine Beseitigung des Fehlers nicht schon mit einfachen Hinweisen und gemeinsamen Anstrengungen geschafft worden ist. Um es kurz zu sagen: Mängel, die zu einer Beanstandung und zu einer Stellungnahme der Intendantin hätten führen müssen, gab es nicht. Auch die damit notwendige Einbeziehung des Verwaltungsrates konnte damit unterbleiben. Eine Unterrichtung der Gremien erfolgt damit durch diesen Tätigkeitsbericht, der den Versuch unternimmt, einen Einblick in die Tätigkeit des Rundfunkdatenschutzbeauftragten im MDR insgesamt zu geben.

Die Datenschutzaufgaben beim MDR werden nicht nur von dem Rundfunkdatenschutzbeauftragten, sondern ebenso auch vom Datenschutzbeauftragten gemäß Artikel 37 DSGVO, dem betrieblichen Datenschutzbeauftragten, erfüllt. Dieses Amt wird von Herrn Matthias Meincke wahrgenommen, für dessen vertrauensvolle Zusammenarbeit ich mich bedanken und unsere gemeinsamen Anstrengungen für die Sache des Datenschutzes ausdrücklich würdigen möchte. Bereits von Anfang an hat sich diese Zusammenarbeit fruchtbar und kollegial gestaltet, und ich glaube, dass wir auch in dem rollengerechten Zusammenwirken gute Ergebnisse für den Datenschutz beim MDR erreicht haben. Herr Dr. Bernd Appel ist weiterhin stellvertretender betrieblicher Datenschutzbeauftragter, und nach wie vor ist die Zusammenarbeit sehr angenehm. Als Ansprechpartner und kompetenter Datenschutzexperte hat er gute Arbeit geleistet.

Nach § 40 Abs. 1 Satz 6 MDR-Staatsvertrag gelten die Vorschriften zur journalistischen Datenverarbeitung auch für Hilfs- und Beteiligungsunternehmen des MDR. Der Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Datenschutzvorschriften bei der Tätigkeit des MDR auch bei der Tätigkeit seiner Beteiligungsunternehmen im Sinne von § 16c Abs. 3 Satz 1 Rundfunkstaatsvertrag. Damit bin ich auch als Aufsicht über die Mehrheitsbeteiligungen des MDR verantwortlich. Hier findet ein regelmäßiger Austausch mit den dort zuständigen betrieblichen Datenschutzbeauftragten statt. Neben der allgemeinen Erörterung von Rechtsfragen hatten wir auch einen Vorfall zu bearbeiten. Darüber wird in Kapitel 7.1 berichtet.

Die Überwachung des Kinderkanals obliegt nach bisherigem Verständnis auch dem Rundfunkdatenschutzbeauftragten des MDR. Da es sich um eine Gemeinschaftseinrichtung handelt, könnte hier auch die Auffassung vertreten werden, dass sämtliche Rundfunkdatenschutzbeauftragten von ARD und ZDF (als Träger dieser Einrichtung) zuständig sind. Die Rundfunkdatenschutzkonferenz (RDSK), der Zusammenschluss der spezifischen Aufsichtsbehörden, hat sich jedoch entschieden, hier das Federführungsprinzip anzuwenden. Eine entsprechende Übereinkunft wird jedoch noch diskutiert und ist im Berichtszeitraum nicht abgeschlossen worden.

Dennoch muss die Arbeit gemacht werden, und Herr Meincke und ich arbeiten an dieser Stelle sehr eng mit Herrn Jörn Voss zusammen, der bereits seit vielen Jahren als betrieblicher Datenschutzbeauftragter des Kinderkanals beste Arbeit leistet. Ihm gebührt deshalb besonderer Dank.

Ende des Jahres 2018 endete auch meine Zeit als Vorsitzender des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB). Zu meinem Nachfolger wurde Herr Dr. Heiko Neuhoff bestimmt, Rundfunkdatenschutzbeauftragter des NDR. Im Jahr 2019 wurde überdies die Rundfunkdatenschutzkonferenz gegründet, der Zusammenschluss der unabhängigen Aufsichtsstellen über den öffentlich-rechtlichen Rundfunk in Deutschland. Hier gibt es auch neue Akteure und Akteurinnen, und die für uns alle noch neue Rolle hat dazu geführt, dass intensiv über Aufgaben der Aufsicht und spezifische Pflichten diskutiert wurde. Wie immer, wenn sich etwas Neues ergibt, kann man von einer spontanen Einigkeit nicht ausgehen. Gerades deshalb bin ich sehr froh, dass wir uns darauf verständigt haben, ein entsprechendes Gremium zu gründen und gleichzeitig die Zusammenarbeit im AK DSB mit den betrieblichen Datenschutzbeauftragten aufrecht zu erhalten. Ich glaube, dass sowohl aufsichtsrechtliche Fragen von der behördlichen Position beleuchtet werden sollten, als auch die tägliche „Datenschutzarbeit“ von den betrieblichen Datenschutzbeauftragten gemeinsam mit den Rundfunkdatenschutzbeauftragten zu leisten ist. Die Aufgaben werden nicht weniger, Datenschutz ist als Thema omnipräsent und nach wie vor sehr wichtig, sodass auch die Zukunft spannende Probleme und Aufgaben für uns Datenschützerinnen und Datenschützer bereithalten wird. Nach wie vor empfinde ich die Arbeit als bereichernd und herausfordernd. Gerade die Tätigkeit als Aufsicht hält neue Aspekte bereit. Hier gilt es eine klare Rolle einzunehmen. Ich bin dankbar, dass ich diese besondere Tätigkeit ausüben darf und freue mich auf die nächsten Jahre.

2. Aufgaben des Rundfunkdatenschutzbeauftragten

2.1 Aufgaben und Befugnisse

Nach § 42 Abs. 1 des MDR-Staatsvertrages ernennt der MDR einen Rundfunkbeauftragten für den Datenschutz beim MDR, der zuständige Aufsichtsbehörde im Sinne der DSGVO ist. Eine Ernennung erfolgt durch den MDR-Rundfunkrat mit Zustimmung des Verwaltungsrates für die Dauer von vier Jahren. Das Amt des Rundfunkdatenschutzbeauftragten ist vor allem geprägt durch seine Unabhängigkeit, er unterliegt keiner Rechts- oder Fachaufsicht. Die vom Verwaltungsrat ausgeübte Dienstaufsicht darf seine Unabhängigkeit keinesfalls beeinträchtigen. Der Rundfunkdatenschutzbeauftragte ist damit anstelle der oder des Landesbeauftragten für den Datenschutz Aufsichtsbehörde nach Art. 51 DSGVO. In dieser Funktion ist er zuständig für die Einhaltung des Datenschutzes beim MDR und seiner gesamten Tätigkeit, aber auch bei seinen Beteiligungsunternehmen. Die Aufgaben und Befugnisse ergeben sich aus § 42 MDR-Staatsvertrag, aber auch aus den Artikeln 57 und 58 DSGVO. Jeder hat das Recht, sich unmittelbar an den Rundfunkdatenschutzbeauftragten zu wenden, wenn man der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch den MDR oder seiner Beteiligungsunternehmen in seinen schutzwürdigen Belangen verletzt zu sein. Dies entspricht in etwa den Aufgaben nach Artikel 57 DSGVO, wonach die Datenschutzgrundverordnung zu überwachen und durchzusetzen ist. Dort ist auch geregelt, dass er an der Sensibilisierung der Verantwortlichen, der betroffenen Personen und der Öffentlichkeit mitzuwirken hat, und postuliert ebenso die Pflicht, mit anderen Aufsichtsbehörden zusammenzuarbeiten. Dies wird umgesetzt mit der Zusammenarbeit mit den anderen Rundfunkdatenschutzbeauftragten in der Rundfunkdatenschutzkonferenz RDSK (siehe dazu auch Kapitel 9) sowie mit der Teilnahme an Sitzungen der Datenschutzkonferenz, in der sich die staatlichen Datenschutzbeauftragten in Deutschland zusammengeschlossen haben. Hier ist eine Zusammenarbeit nicht immer ganz einfach, denn die staatlichen Datenschutzbeauftragten legen zuweilen nicht allzu großen Wert auf eine enge Zusammenarbeit bei gemeinsam interessierenden Themen. Die hoheitlichen Befugnisse einer Aufsichtsbehörde, zu der der Rundfunkdatenschutzbeauftragte zählt, sind im Artikel 58 DSGVO geregelt. Danach kann ein Verantwortlicher (der MDR oder seine Beteiligungsunternehmen) ggf. per Verwaltungsakt zu Handlungen oder Unter-

lassungen verpflichtet werden, insbesondere können Verarbeitungsvorgänge auch untersagt werden. Das Gesetz unterscheidet hier zwischen Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen und beratenden Befugnissen. Geldbußen gegenüber dem MDR kann der Rundfunkdatenschutzbeauftragte allerdings nicht verhängen (§ 42b Abs. 1 MDR-Staatsvertrag). Dies betrifft jedoch nicht die Beteiligungsunternehmen, gegenüber jenen sind Bußgelder möglich. Die Datenschutzgrundverordnung sieht überdies vor, dass zwischen Aufsicht und betrieblichem Datenschutz zu trennen ist. Dies bedeutet aber nicht, dass eine enge Zusammenarbeit nicht möglich wäre. Im Gegenteil, die DSGVO sieht hier ein enges Zusammenwirken vor, das – so mein Eindruck – beim MDR in besonders guter Weise funktioniert. Nach meiner Auffassung darf sich die Aufsicht nicht darauf beschränken „von außen" auf das Datenschutzgeschehen des MDR zu blicken, sondern ich sehe mich dazu verpflichtet, an und in den Datenschutzprozessen mitzuwirken und in diesbezügliche Entscheidungen eingebunden zu sein.

2.2 Voraussetzungen für die Bearbeitung einer Beschwerde

Im Sommer 2019 erreichte mich eine Beschwerde zu der Ausgestaltung des Sommerinterviews im MDR Landesfunkhaus Thüringen. Im Zuge dieser Aktion konnten interessierte Bürgerinnen und Bürger ihre Fragen an die Kandidaten der Landtagswahl in Thüringen senden, die dann im Rahmen eines Sommerinterviews gestellt worden sind. Bei Fragen, die aus zeitlichen Gründen nicht berücksichtigt werden konnten, bestand die Möglichkeit, diese an den Kandidaten weiterzuleiten. Hier war vorgesehen, auch die Kontaktdaten des Fragestellers weiterzuleiten, damit ggf. eine direkte Antwort erfolgen konnte. In der Tat war die Ausgestaltung der Einwilligungserklärung unter datenschutzrechtlichen Gesichtspunkten nicht einwandfrei, sodass ich an dieser Stelle eingreifen musste. Interessant ist in diesem Zusammenhang jedoch vor allem, dass der Beschwerdeführer oder die Beschwerdeführerin, seine oder ihre Identität geheim halten wollte. Selbstverständlich werden auch anonyme Beschwerden bearbeitet - so war es auch in diesem Fall. Erwartet und wünscht der Beschwerdeführer oder die Beschwerdeführerin eine Antwort, so hat er oder sie ihre Identität aufzudecken, und das aus folgenden Erwägungen:

Eine Beschwerde ist gemäß der gesetzlichen Vorgaben durch eine betroffene Person einzulegen. Sie hat einen Sachverhalt vorzutragen, der die Möglichkeit einer Rechtsverletzung begründet. Nicht indes ist der Nachweis erforderlich, dass die Daten der Person tatsächlich verarbeitet werden. Allerdings muss die beschwerende Person mit der in Rede stehenden und bemängelten Datenverarbeitung in einem unmittelbaren Zusammenhang stehen und gerade durch diese identifizierbar sein. Das Beschwerderecht gegenüber dem Rundfunkdatenschutzbeauftragten dient dem individuellen Rechtsschutz und nicht der objektiven Durchsetzung des europäischen Datenschutzrechts. Damit kann der konkrete Verstoß gegenüber der anonym zu bleiben wünschenden Person nur in allgemeiner Hinsicht kommentiert werden und natürlich der Datenschutzfehler beseitigt werden. Nicht jedoch kann eine Abhilfe der Beschwerde veranlasst werden. Hintergrund ist, dass eine konkrete Beschwerde durch Verweigerung der Identifizierung nicht glaubhaft gemacht werden kann.

Der Beschwerdeführerin oder dem Beschwerdeführer habe ich in dieser Weise geantwortet und versichert, dass bei Übersendung ihrer oder seiner Daten an mich als Rundfunkdatenschutzbeauftragten eine strenge Zweckbindung im Hinblick auf seine Beschwerde garantiert würde. Jedoch habe ich darauf keine Antwort erhalten und damit den Vorgang abgeschlossen.

2.3 Eingaben beim Rundfunkdatenschutzbeauftragten

Der Rundfunkdatenschutzbeauftragte ist Aufsichtsorgan über die Datenverarbeitung beim MDR. Im Zuge dessen ist er nicht zuständig für die Erteilung von Auskunftsersuchen, sondern dafür da, bei Beschwerden tätig zu werden. Im Berichtszeitraum sind dennoch vier Auskunftsersuchen direkt bei mir eingegangen, die ich jedoch an den MDR bzw. dem Zentralen Beitragsservice zur Bearbeitung weiter gegeben habe.

Oftmals wenden sich Petentinnen und Petenten fälschlicherweise an die Landesbehörden von Sachsen, Sachsen-Anhalt und Thüringen oder aber auch an den Bundesdatenschutzbeauftragten, wenn sie sich über die Datenverarbeitung hinsichtlich des Beitragseinzugs beschweren wollen. Diese Beschwerden werden

dann von den Behörden an mich weitergereicht und von meiner Seite aus bearbeitet. Im Berichtszeitraum erreichten mich neun solcher Beschwerden.

Der richtige Weg ist natürlich, sich direkt an mich zu wenden. Im Zeitraum des Berichtes erreichten mich insgesamt 19 direkte Beschwerden, die vollständig abgearbeitet werden konnten. Nicht immer ist es möglich, zur vollen Zufriedenheit der Petentinnen und Petenten zu antworten. Oftmals aber ist festzustellen, dass sich die Beschwerden in grundsätzlicher Hinsicht gegen die Beitragspflicht wenden. Der Datenschutz wird nach meiner Erfahrung in solchen Fälle eher vorgeschoben.

Insgesamt ist festzuhalten, dass die Neigung zu datenschutzrechtlichen Beschwerden nicht sehr hoch ist. Dies ist sicherlich darauf zurückzuführen, dass die Datenverarbeitung beim Beitragseinzug einer strengen gesetzlichen Zweckbindung unterliegt und daher eine hohe Akzeptanz erfährt, jedoch auch darauf, dass das Datenschutzmanagement sowohl beim MDR als auch beim Zentralen Beitragsservice den Anforderungen entspricht.

3. Entwicklung des Datenschutzrechts im Jahr 2019

Die EU-Datenschutzgrundverordnung (DSGVO) ist bereits seit dem 25.05.2018 wirksam. Aufgrund der neuen Rechtsmaterie waren und sind Einzelheiten der Umsetzung bis heute offen und umstritten. Es gibt in verschiedenen Bereichen weder eine einheitliche Auffassung der Aufsichtsbehörden noch eine gesicherte Rechtsprechung. Auch die Umsetzung der erforderlichen Anpassung einer Vielzahl von Bundes- und Landesgesetzen an die DSGVO ist nicht abgeschlossen. Soweit sie den MDR betrifft, soll die Rechtsentwicklung kurz dargestellt werden.

3.1 Europäische Entwicklungen

Der Europäische Datenschutzausschuss (Artikel 68 DSGVO) hat die Aufgabe, die einheitliche Anwendung der DSGVO sicherzustellen. Er hat zwar schon viele Papiere veröffentlicht, jedoch ist es bislang nicht gelungen, einheitliche Kriterien z.B. für die Datenschutzfolgeabschätzung auf europäischer Ebene zu entwickeln.

Der Europäische Gerichtshof (EuGH) spielt ebenso eine wichtige Rolle bei der Auslegung der Datenschutzgrundverordnung. Im Jahr 2019 hat sich der EuGH in seinen Urteilen mit der gemeinsamen Verantwortlichkeit mehrerer Datenverarbeiter (Artikel 26 DSGVO), der Einbindung von Plugins bzw. „Gefällt-mir-Buttons“ und der Einwilligung in die Verwendung von Cookies beschäftigt und leistet damit Beiträge zur einheitlichen Auslegung der DSGVO.

Die ePrivacy-Verordnung soll als Ersatz der Richtlinie 2002/58/EG zur elektronischen Kommunikation fungieren. Regelungsmaterie sollen Vorgaben zum Datenschutz bei der Bereitstellung und Nutzung von Telemediendiensten, klassischen Kommunikationsdiensten wie Telefonie und SMS, aber auch von internetbasierte Kommunikationsdienste, insbesondere Messengern wie Skype oder WhatsApp sein. Ursprünglich war geplant, gleichzeitig mit Einführung der DSGVO auch die ePrivacy-Verordnung in Kraft zu setzen und zu veröffentlichen. Leider ist dies bis heute nicht gelungen. Dies wäre insbesondere für eine rechtsichere Einbindung von Trackingverfahren und Cookies sehr sinnvoll, denn dies würde auch die umstrittene Anwendung des Telemediengesetzes (TMG) als deutsche Rechtsmaterie ablösen. Die Regelungen des Telemediengesetzes gibt es zwar noch, aber dieses soll nach Auffassung der staatlichen Aufsichtsbehörden gar nicht mehr anwendbar sein. Leider gibt es keine verlässliche Information darüber, wann eine Einigung über die ePrivacy-Verordnung zu erwarten ist. Dies ist vor allem misslich, weil man sich in einen Bereich Rechtsklarheit erhofft, der höchst umstritten ist. Insbesondere im Hinblick auf Trackingverfahren und Cookies gibt es trotz der neuesten Rechtsprechung noch viele Unsicherheiten. Hier sind Rechtsentwicklungen zu erwarten, die hoffentlich bald Klarheit schaffen.

3.2 Gesetzgebung im Bereich des Bundes

Die Anpassung deutscher Gesetze an die DSGVO wurde mit dem 2. Datenschutzanpassungs- und Umsetzungsgesetz EU vom 20.11.2019 fortgesetzt. Neben 154 Fachgesetzen wurde auch wieder das Bundesdatenschutzgesetz (BDSG) geändert und zwar in folgenden Punkten:

- Die Schwelle zur Bestellung eines betrieblichen Datenschutzbeauftragten bei nichtöffentlichen Stellen wurde in § 38 BDSG von 10 auf 20 Personen

erhöht. Dies schafft zwar eine gewisse Vereinfachung, ändert aber nichts daran, dass nach wie vor eine Fülle von datenschutzrechtlichen Pflichten für kleine Unternehmen und auch z. B. Vereine bestehen.

- Die Aufsichtsbefugnisse des Bundesdatenschutzbeauftragten wurden nicht nur gestärkt, sondern auch auf den Verwaltungsbereich der Deutschen Welle ausgedehnt. Dies ist im Hinblick auf die Staatsferne des öffentlich-rechtlichen Rundfunks ein Rückschritt und wird von den Rundfunkdatenschutzbeauftragen kritisch gesehen.
- Mit Änderung des § 22 BDSG wird eine Weitergabe sensibler Informationen im Rahmen von Präventions- und Deradikalisierungsprogrammen an Sicherheitsbehörden ermöglicht werden.
- Beim Beschäftigtendatenschutz (§ 26 BDSG) ist jetzt festgehalten, dass die Einwilligung in eine Datenverarbeitung zukünftig auch elektronisch erfolgen kann.
- Die Zulässigkeit der Verarbeitung von Daten zu Zwecken staatlicher Auszeichnungen und Ehrungen wird durch einen neuen § 86 BDSG geregelt.

3.3 Gesetzgebung im Bereich der Zuständigkeit der Länder

Die Datenschutzgrundverordnung gilt unmittelbar, ist also ohne weitere Umsetzungsakte gültig. Allerdings gibt es nach wie vor auch weitere bundes- oder landesrechtliche Vorschriften über den Datenschutz. Im Bund ist dies das Bundesdatenschutzgesetz. In Sachsen ergänzt insbesondere das Sächsische Datenschutzdurchführungsgesetz die Datenschutzgrundverordnung um allgemeine datenschutzrechtliche Regelungen. Hintergrund ist, dass Vorschriften, die sich im bisherigen Sächsischen Datenschutzgesetz bewährt haben, auch zukünftig beibehalten werden sollen. Über § 39 des MDR-Staatvertrages ist die Anwendung des Sächsischen Datendurchführungsgesetzes für den MDR eröffnet. Dort ist u.a. geregelt, dass die Verarbeitung personenbezogener Daten zulässig ist, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen (hier MDR) liegenden Aufgaben erforderlich ist. Damit ist ein weiter Spielraum für alle Datenverarbeitungen gegeben, die der MDR in Erfüllung seiner Aufgabe durchführen muss. Ebenso enthält das Gesetz Regelungen zum Beschäftigtendatenschutz, die auch für den MDR gelten und die Rechtsanwendung insoweit erleichtern. Hintergrund ist, dass

die DSGVO in Artikel 88 Öffnungsklauseln vorgesehen hat, die eine nationale Rechtssetzung zum Beschäftigtendatenschutz ermöglichen.

3.4 MDR-Staatsvertrag

Bereits im Jahr 2018 wurde auch der MDR-Staatsvertrag an die Datenschutzgrundverordnung angepasst. Hier wurden insbesondere die Vorschriften zum Medienprivileg und die Einführung des Rundfunkdatenschutzbeauftragten neu gefasst. In meinem letzten Tätigkeitsbericht für den Zeitraum 01.07.2016 bis 31.07.2018 habe ich unter den Punkten 1. und 2. hierzu ausführlich berichtet. Daher soll an dieser Stelle auf Wiederholungen verzichtet werden.

3.5 22. Rundfunkänderungsstaatsvertrag

Am 01.05.2019 ist der 22. Rundfunkänderungsstaatsvertrag (RÄndStV) in Kraft getreten. Er hat vor allem die zeitgemäße Ausweitung des Telemedienauftrages des öffentlich-rechtlichen Rundfunks zum Gegenstand. Die Kernpunkte der Novellierung betreffen die Herstellung eigenständiger audiovisueller Inhalte für die Online-Verbreitung, das Angebot der Inhalte auch außerhalb des dafür jeweils eingerichteten Portals, die Neureglung zur Feststellung presseähnlicher Telemedien sowie die Erweiterung des Umfangs von Telemedienkonzepten. Dies hat insoweit Auswirkungen auf den Datenschutz, weil sich am Auftrag auch das Medienprivileg messen lassen muss. Ebenso stellt sich aber gerade im Zusammenhang mit der Verarbeitung von Nutzerdaten die Frage, in welchem Zusammenhang auch jenseits des Medienprivilegs die Verarbeitung dieser Daten zur Auftragserfüllung herangezogen werden dürfen. Dies spielt insbesondere bei Fragen zur Online-Nutzungsmessung eine Rolle und muss im jeweiligen Einzelfall entschieden werden.

3.6 23. Rundfunkänderungsstaatsvertrag

Am 01.06.2020 ist der 23. Rundfunkänderungsstaatsvertrag in Kraft getreten. Er wurde auf der Ministerpräsidentenkonferenz im Oktober 2019 unterzeichnet. Schwerpunkte dieses Änderungsstaatsvertrages sind zum einen die Umsetzung

der Vorgaben des BVerfG zur Befreiung der Rundfunkbeitragspflicht für Zweitwohnungsinhaber und zum anderen die Einführung eines regelmäßigen alle vier Jahre stattfindenden Meldedatenabgleichs. Bezüglich der personenbezogenen Daten ist eine klare Zweckbindung vorgegeben, ebenso sind nicht erforderliche Daten unverzüglich zu löschen. Sofern die Kommission zur Ermittlung des Finanzbedarfs (KEF) im Rahmen ihrer Berichte feststellt, dass der Datenbestand der Landesrundfunkanstalten hinreichend aktuell ist, soll der regelmäßige Meldedatenabgleich nicht durchgeführt werden. Mit diesem Instrument ist beabsichtigt, den Ausgleich zwischen der Beitragsgerechtigkeit einerseits und dem Recht auf informationelle Selbstbestimmung andererseits herzustellen. Weitere Anpassungen sind Folgeänderungen aufgrund der Vorgaben der DSGVO. Unter anderem wird der Umfang des datenschutzrechtlichen Auskunftsanspruchs insoweit konkretisiert, dass es dem Massenverfahren unter Berücksichtigung des Artikels 23 DSGVO beim Zentralen Beitragsservice gerecht wird.

Der Arbeitskreis der Datenschutzbeauftragten des öffentlich-rechtlichen Rundfunks (AK DSB) vertritt die Auffassung, dass es sich bei dem vorgesehenen regelmäßigen Meldedatenabgleich nicht um eine unzulässige Vorratsdatenspeicherung handele. Zu einer angestrebten Vermeidung eines Vollzugsdefizits und zur Herstellung größerer Beitragsgerechtigkeit ist er auch unter Berücksichtigung der datenschutzrechtlichen Aspekte geeignet und verhältnismäßig.

3.7 Entwurf des neuen Medienstaatsvertrages

Am 05.12.2019 haben die Ministerpräsidenten der Länder den neuen Medienstaatsvertrag verabschiedet. Dieser löst den Rundfunkstaatsvertrag ab, der nur für ausgewählte Medienformen Regelungen vorsah. Nunmehr sollen auch für Online-Anbieter wie Google und Facebook künftig wichtige Grundsätze des Medienrechtes unmittelbar gelten. Reformiert werden soll u.a. die Zulassungspflicht für Rundfunkangebote. Bisher gab es immer wieder Unstimmigkeiten, weil z. B. Anbieter von Live-Streaming Angeboten mit mehr als 500 gleichzeitigen Zuschauern Lizenzen brauchten. Künftig sollen solche Anbieter keine Zulassung benötigen, wenn sie im Durchschnitt weniger als 20.000 gleichzeitige Nutzerinnen und Nut-

zer erreichen oder nur eine geringe Bedeutung für die individuelle und öffentliche Meinungsbildung entfalten. Ferner wird der Begriff „Medienintermediäre“ eingeführt. In diese Sparte fallen Plattformen wie Google und Facebook. Aber auch für Sprachassistenten und smarte Lautsprecher wie die Amazon-Technologie „ALEXA“ sollen künftig Regelungen des Staatsvertrages gelten. Im Hinblick auf den Datenschutz sind diese Vorgaben interessant, denn auch hier wird sich zeigen, inwieweit das Institut des Medienprivilegs auf die verschiedenen Formen der Angebote ausstrahlt.

4. Datenschutz beim MDR

4.1 Verantwortung für Facebook Fanpages

Der Europäische Gerichtshof (EuGH) hat bereits im Juni 2018 entschieden, dass Fanpagebetreiber gemeinsam mit Facebook Verantwortung tragen für die dort stattfindende Datenverarbeitung. Das bedeutet nicht zwangsläufig, dass der Fanpagebetreiber für die gesamte Datenverarbeitung von Facebook voll verantwortlich ist, sondern für den Teil, über den er hinsichtlich der Zwecke und Mittel (mit-) entscheidet. Wenn eine solche gemeinsame Verantwortung vorliegt, muss gemäß der DSGVO ein Vertrag geschlossen werden, darüber, wie die gemeinsame Verantwortung verteilt ist und wer die Pflichten aus der DSGVO übernimmt. Nun lässt es sich nicht realisieren, dass jeder Fanpagebetreiber einen Einzelvertrag mit Facebook verhandelt, sondern Facebook ist den Weg gegangen, ein sogenanntes Addendum bereitzustellen, das die datenschutzrechtliche Verantwortlichkeit und die jeweils daraus erwachsenen Pflichten regelt. Dies ist ein praktikabler Ansatz, damit nicht jeder Betreiber einen gesonderten Vertrag zu schließen hat. Facebook erkennt darin seine primäre Verantwortlichkeit an, was auch in Ordnung ist. Der EuGH hat festgestellt, dass die Akteurinnen und Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und unterschiedlichem Ausmaß in der Weise einbezogen sein können, dass der Grad der Verantwortlichkeit eines jeden unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.

Der MDR nutzt keine direkt auf eine Person zurückzuführenden personenbezogenen Daten, sondern bezieht Daten von Facebook nur aggregiert und in anonymer Form. Ihn interessiert im Wesentlichen, ob sein auf Facebook bereit gestelltes Angebot (das im Übrigen seinem Auftrag entspricht) auch tatsächlich von den Nutzerinnen und Nutzern angenommen wird.

Das Bundesverwaltungsgericht hat am 11.09.2019 die Entscheidung des EuGH bestätigt und festgestellt, dass datenschutzrechtliche Aufsichtsbehörden dem Betreiber einer Fanpage den Betrieb untersagen können. Auch wurde der Ausgangsrechtsstreit an die Vorinstanz zurückverwiesen. Hier stand im Berichtszeitraum noch die Entscheidung aus, ob das Betreiben von Fanpages aufgrund von etwaigen Datenschutzverstößen rechtswidrig war und ist. Der MDR agiert auf Basis des Facebook Addendums und informiert über die Datenverarbeitung in seinen Datenschutzerklärungen. Er verarbeitet selbst keine personenbezogenen Daten, und über Facebook werden nur Menschen erreicht, die freiwillig die Angebote von Facebook nutzen. Ebenso sind die Facebook-Angebote redaktionell-journalistisch und fallen daher unter das datenschutzrechtliche Medienprivileg. Nicht vergessen darf aber auch, dass nicht transparent ist, was Facebook tatsächlich mit den Daten macht. Zunächst bleibt abzuwarten, was die deutschen Gerichte hinsichtlich der rechtskonformen Verarbeitung von Daten bei Facebook im Konkreten entscheiden und sodann ist abzuwägen, ob das journalistische Interesse an der Datenverarbeitung bei Facebook den dort herrschenden etwaigen Mängeln in der Transparenz überwiegt. Bereits im Juni 2019 hat das Land Sachsen-Anhalt entschieden, sich vollständig aus Facebook zurückzuziehen. Die Landesdatenschutzbeauftragten sind mehrheitlich der Auffassung, dass den Behörden anzuraten sei, sozialen Netzwerken den Rücken zu kehren, eben weil die dort betriebene Datenverarbeitung letztendlich nicht transparent und klar sei. Im Hinblick auf die publizistische Zielrichtung der Nutzung von Drittplattformen durch den MDR und das insoweit geltenden Medienprivileg halte ich einen Rückzug des MDR aus Facebook für nicht erforderlich.

Ein weiteres Urteil des EuGH vom Juli 2019 hat ebenfalls das Thema Datenschutz und Facebook beleuchtet. In diesem Fall ging es um den sogenannten „Like-Button“. Das ist ein Programmcode von Facebook, der von Webseitenbetreibern

als sogenanntes Plugin eingebunden wird. Das hat zur Folge, dass bei jedem Aufruf einer Internetseite, die ein solches Plugin enthält, automatisch Daten an den Anbieter des Plugins übertragen werden. Eine Betätigung des Buttons ist dafür nicht erforderlich. In dieser Entscheidung hat der EuGH klargestellt, dass der Websitebetreiber, der das Plugin einbettet, nur für die Erhebung von Daten und Weitergabe an Facebook verantwortlich ist, nicht jedoch für die Datenverarbeitung bei Facebook. Dessen ungeachtet haben die Datenschutzbeauftragten von ARD und ZDF bereits im Jahr 2016 erkannt, dass die Einbettung eines solchen Plugins und damit die Datenweitergabe an Facebook, ohne dass die Nutzer aktiv dazu beitragen, mehr als bedenklich ist. Es wurde die sogenannte Zwei-Klick-Lösung empfohlen und auch umgesetzt. Zwar erscheint der Like-Button beim Aufruf der Website, jedoch muss die Nutzerin bzw. der Nutzer ihn aktiv betätigen, um mit Facebook verbunden zu werden. Auch hier bestehen datenschutzrechtliche Unsicherheiten, weshalb die Praxis beim MDR dahingehend geändert wurde, dass eine Verbindung zu Facebook nur durch einen in jeglicher Hinsicht unproblematischen Link gewährleistet ist. Das Thema Facebook und Drittplattformen wird uns datenschutzrechtlich sicherlich noch einige Zeit beschäftigen. Solange nicht wirklich klar ist, wie rechtlich mit den in den USA beheimaten Anbietern umzugehen ist, werden die Diskussionen nicht abreißen. Dass der MDR im Rahmen seines Auftrages auch solche Plattformen mit Inhalten bedienen darf, steht außerhalb des Datenschutzrechtes außer Frage und muss in diesem Kontext auch immer in die Gewichtung einbezogen werden.

4.2 Kooperation Altersvorsorge

Im Sommer 2019 hat der MDR eine Aktion „Check: Altersvorsorge“ durchgeführt. Der MDR beabsichtigte in seinen Sendungen „MDR um 4“und „Umschau“ auf das Thema Altersvorsorge hinzuweisen und interessierten Zuschauerinnen und Zuschauern die Möglichkeit zu eröffnen, ihre Altersvorsorge zu überprüfen. Zu diesem Zweck sollte ein Online-Formular bereitgestellt werden, in dem die Interessenten ihre Daten eintragen konnten, die dann an die Verbraucherzentralen weitergeleitet werden sollten. Dort wiederum sollte ein rechtlich selbständiger Vertrag zur Beratung über die Altersvorsorge geschlossen werden. Aus datenschutz-

rechtlicher Sicht war zu bewerten, dass Daten vom MDR an die Verbraucherzentralen weitergereicht werden. Auch war die Frage zu beantworten, wie über dieses Thema in den Sendungen des MDR berichtet werden konnte. Der betriebliche Datenschutzbeauftragte und ich haben daher gemeinsam ein Verfahren entworfen, das allen Anforderungen gerecht wird:

Zunächst musste eine Einwilligung eingeholt werden, um die Daten an die Verbraucherzentralen weiterzuleiten. Damit der MDR im Anschluss an die erfolgte Beratung über die Ergebnisse des „Checks: Altersvorsorge“ berichten konnte, mussten die Verbraucherzentralen gesondert um das Einverständnis der Teilnehmerinnen und Teilnehmer bitten, ihre insoweit erweiterten Daten (Ergebnisse aus dem Beratungsgespräch) an den MDR zu übermitteln. Die Berichterstattung erfolgte ohne den Bezug zu den Personen und konzentrierte sich auf die Ergebnisse. Wenn der MDR allerdings über einzelne Personen zu berichten beabsichtigte, wurden diese vorher vom MDR kontaktiert und gesondert um ihre Einwilligung gebeten.

An diesem Beispiel ist gut zu erkennen, dass Datenschutzrecht und Programmrecht teilweise eng verzahnt sind und eine saubere rechtliche Konstruktion kompliziert sein kann. In diesem Fall war es aber wichtig, darauf zu achten, transparent darzustellen, wie die Datenverarbeitung beim MDR einerseits und bei den Verbraucherzentralen andererseits abläuft, um den interessierten Zuschauerinnen und Zuschauern auch klar vor Augen zu führen, dass die Verarbeitung ihrer personenbezogenen Daten streng zweckbezogen und nur in der notwendigen Art und Weise erfolgt. Auch ist eine schnelle und enge Abstimmung mit den redaktionellen Bereichen gut geglückt.

4.3 mdrFRAGT

Ausgehend von der strategischen Zielstellung, einen gesellschaftlichen Dialog zu führen, wurde „mdrFRAGT – das Meinungsbarometer für Mitteldeutschland“ initiiert. Dabei handelt es sich um ein Umfragetool, mit Hilfe dessen sich registrierte Nutzerinnen und Nutzer an Umfragen zu tagesaktuellen Themen beteiligen können. Zu diesem Zweck sollte ein Dienstleister aus den Niederlanden (Vision Critical) beauftragt werden.

Neben den allgemeinen Fragen, wie z. B ein sogenannter Auftragsverarbeitungsvertrag geschlossen werden kann, musste geklärt werden, in welchem Umfang Nutzerdaten für die Anmeldung erforderlich sind. Um ein möglichst genaues Meinungsbild zu erfragen und auch zu wissen, aus welchen regionalen und sozialen Bereichen die Teilnehmerinnen und Teilnehmer kommen, sind bei der Anmeldung relativ viele Daten anzugeben. Die Namen und Adressen gehören jedoch nicht dazu, sodass ein Rückschluss auf einzelne Personen nicht beabsichtigt und im Regelfall auch nicht möglich ist. Dennoch erfordert eine solche Anmeldung sowohl größte Transparenz, d.h. umfassende Aufklärung über den Sinn und Zweck der Datenverarbeitung, als auch ein hohes Maß an Datensicherheit, das über technisch organisatorischen Maßnahmen zusammen mit dem beauftragten Dienstleister sichergestellt wird. Gemeinsam mit dem betrieblichen Datenschutzbeauftragten habe ich mit der verantwortlichen Redaktion beraten und empfohlen, wie das Verfahren auszusehen hat und wie die Informationen für die Nutzerinnen und Nutzer so aufbereitet werden, dass lückenlose Informationen vorliegen. Die Maßstäbe an die Einwilligung zur Datennutzung durch den MDR entsprechen der gesetzlichen Vorgabe, sodass man jederzeit seine Teilnahme an dem Umfragetool widerrufen kann. Ebenso ist über ein sogenanntes Double-Opt-In Verfahren sichergestellt, dass tatsächlich keine missbräuchlichen Anmeldungen möglich sind: Erst die Bestätigung einer vom MDR versandten E-Mail kann eine Teilnahme an dem Tool ermöglichen. Dieses Verfahren ist Standard und sorgt für zusätzliche Sicherheit. Durch das journalistische Medienprivileg ist die Datenverarbeitung für journalistische Zwecke relativ frei. Daher ist gerade das Tool Vision Critical und das Angebot mdrFRAGT ein gutes Beispiel dafür, dass der Datenschutz dennoch nicht aus dem Blick verloren werden darf. Zwar sind Daten zur journalistischen Verwendung von dem Regime des Datenschutzrechtes in vielerlei Hinsicht befreit, jedoch betrifft dies nicht die im vorliegenden Fall anfallenden Nutzerdaten. Diese müssen streng nach der Datenschutzgrundverordnung und allen anderen Gesetzen verarbeitet werden und unterliegen einer eindeutigen Zweckbindung. Nach meiner Auffassung ist es in diesem Fall sehr gut gelungen, den datenschutzrechtlichen Anforderungen gerecht zu werden. Umso erfreulicher ist, dass das Projekt ein großer Erfolg ist.

4.4 Umfragen mit Civey

Der MDR, namentlich die Online-Redaktion des Landesfunkhauses Magdeburg, hatte den Wunsch, das Umfragetool Civey in die Angebote einzubauen. Civey arbeitet mit verschiedenen Presse- und Medienanbietern zusammen. Ziel ist es nach eigenen Angaben, Menschen Zugang zu repräsentativer Meinungsforschung zu ermöglichen. Repräsentative Ergebnisse sollen durch Online-Befragungen erreicht werden. Wenn man an einer solchen Umfrage teilnehmen will, muss man lediglich Geschlecht, Geburtsjahr und Wohnort angeben. Dies sind zwar personenbezogene Daten, jedoch ist hier eine ausreichende Anonymität deshalb gewahrt, weil keine Namen oder E-Mail-Adressen erhoben werden. Selbstverständlich fällt die IP-Adresse an, die damit einen Rückschluss auf die Person ermöglicht. Dieser Datenweitergabe kann man allerdings jederzeit widersprechen. Auch war es nicht nötig, mit dem Meinungsforschungstool eine sogenannte Auftragsverarbeitungsvereinbarung abzuschließen, da die Datenverarbeitung nicht im Auftrag des MDR, sondern in eigener Verantwortung von Civey durchgeführt wird. Die Tatsache, dass die Datenerhebung in ein Angebot des MDR eingebunden wird, reicht hier nicht aus, um eine gemeinsame Verantwortung zu konstruieren. Auf eine Sache jedoch musste ich hinweisen. Grundsätzlich ist Civey so ausgestaltet, dass die reine Einbettung des Programmcodes in die Angebote des MDR mit Hilfe eines Widgets dazu führt, dass personenbezogene Daten (in diesem Fall die IP-Adresse) der auf der Seite sich befindlichen Nutzer an Civey weitergegeben werden. Dies geschieht, bevor der/die Nutzer/in aktiv auf das Angebot geklickt hat und ist deshalb zu vermeiden, weil eine bewusste Entscheidung des Nutzers bzw. der Nutzerin, mit dem Meinungsforschungsinstitut in Kontakt zu treten, an dieser Stelle nicht möglich ist. Daher musste Sorge dafür getragen werden, dass eine sogenannte Zwei-Klick-Lösung installiert wird. Dies führt dazu, dass eine bewusste Handlung zu dem Zweck ausgeführt wird, überhaupt mit dem Angebot von Civey in Kontakt zu treten. Ob dann tatsächlich an der Umfrage teilgenommen wird, ist einer weiteren freien und informierten Entscheidung vorbehalten.

Die mir bekannt gewordenen Umfragen sind tatsächlich so durchgeführt worden. Insofern konnte hier eine datenschutzfreundliche Lösung umgesetzt werden. Dies ist bei anderen Angeboten von auf dem freien Markt befindlichen Konkurrenten des MDR nicht immer der Fall. Ich bin daher der Auffassung, dass gerade der MDR

gehalten ist, hier besonders vorbildlich zu sein und nicht zu riskieren, dass Daten an andere Verantwortliche weitergeleitet werden, ohne dass die Nutzer dies wissen.

4.5 Zentraler Servicedesk

Im Rahmen der ARD-Strukturreform war beschlossen worden, einen Zentralen Servicedesk für sämtliche ARD-Anstalten und das Deutschlandradio zu etablieren, um Synergien und Einspareffekte zu erzielen. Der Zentrale Servicedesk hat die Aufgabe, eingehende Anfragen und Störmeldungen zu den technischen Systemen auf verschiedenen Wegen systematisch zu erfassen, zu klassifizieren, an die zuständige Stelle weiterzuleiten, zu bearbeiten und zu dokumentieren. Die ARD-Rundfunkanstalten und das Deutschlandradio sind in dem Corporate Network (CN) der ARD über den ARD-Sternpunkt in Frankfurt zusammengeschlossen. Das CN ist eine anstaltsübergreifende Glasfaserinfrastruktur, über die Audio-, Video-, Telefon- und Kommunikationsdaten ausgetauscht werden. Es ist nicht mit dem Internet verbunden und besonders gesichert. Über die Verbindungen des CN soll künftig ein gemeinsamer Zentraler Servicedesk zur Verfügung stehen, der von externen Anbietern betrieben wird.

Der Zentrale Servicedesk soll hauptsächlich über eine zentrale Hotline erreichbar sein und telefonisch Support leisten. Nach einem Telefonanruf erstellt der/die Servicedesk-Agent/in ein Ticket im Zentralen Ticketsystem, in welchem die Störungsmeldung oder die Anfrage eines Anrufers initial erfasst und mit weiteren Informationen angereichert wird. Sofern ein Vorgang beendet und das Ticket geschlossen wird, also das Problem gelöst wurde, ist der Vorgang beendet.

Um diesen Service bereitstellen zu können, werden Dienstleister gebunden, mit denen entsprechende Verträge geschlossen werden müssen. Auch fallen verschiedene personenbezogene Daten an, die hauptsächlich zur Verwaltung der Anfragen und Tickets benötigt werden. Da es sich hierbei um ein ARD-übergreifendes System handelt und damit vergleichsweise große Mengen an Daten verarbeitet werden, wurde zentral beim Bayerischen Rundfunk eine sogenannte Datenschutz-Folgenabschätzung vorgenommen, die sehr genau die Risiken eines solchen Ver-

fahrens betrachtet. Der Rundfunkdatenschutzbeauftragte des NDR sowie ich haben an der Erstellung dieser Folgenabschätzung mitgewirkt und konnten zu einem positiven Ergebnis kommen. Insbesondere musste genau geschaut werden, welche Daten im Einzelnen verarbeitet werden und wie hoch der Schutzbedarf jeweils ist. In diesem Zuge wurde auch festgestellt, dass die Daten unter Umständen einen Rückschluss auf die Sicherheitsarchitektur der Rundfunkanstalten erlauben und Daten in der Cloud verarbeitet werden. Im Zuge dessen wurde bewertet, ob ein legitimer Zweck verfolgt wird und die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge dem entsprechen. Auch wurde das Gebot der Datenminimierung und der datenschutzfreundlichen Voreinstellungen betrachtet und eine Güterabwägung im Sinne des verfolgten berechtigten Interesses vorgenommen. Im Ergebnis überwiegen nach Einschätzung der Datenschutzbeauftragten eindeutig die berechtigten Interessen des Bayerischen Rundfunks bzw. der ARD-Rundfunkanstalten, sodass eine Rechtsgrundlage gegeben war.

Damit konnte eine Freigabe erteilt werden und der Zentrale Servicedesk wurde in Betrieb genommen.

Hervorzuheben ist in diesem Zusammenhang auch, dass zwischen den Landesrundfunkanstalten sogenannte Auftragsverarbeitungsverträge abgeschlossen werden mussten, da hier teilweise technische Probleme durch andere Anstalten gelöst und im Zuge dessen auch personenbezogene Daten bei anderen Anstalten als der eigenen verarbeitet werden. Dies ist im Sinne einer Arbeitsteilung sehr sinnvoll, führt jedoch dazu, dass die einzelnen Anstalten untereinander als Dienstleister fungieren. Somit ist sichergestellt, dass die Datenverarbeitung auch jeweils auf einer stabilen rechtlichen Grundlage fußt und kein „Wildwuchs“ der Datenweiterleitung zwischen den Anstalten herrscht.

In der Praxis hat sich herausgestellt, dass es an der einen oder anderen Stelle noch hakt und insbesondere das Berechtigungskonzept (im Hinblick auf die Sichtbarkeit von Tickets und damit Daten) geschärft und verbessert werden kann. Im Ergebnis hat sich aber gezeigt, dass die Zusammenarbeit in datenschutzrechtlicher Hinsicht auf ARD-Ebene sehr gut funktioniert.

4.6 Risikomanagement für die Verarbeitung von personenbezogenen Daten

Im letzten Tätigkeitsbericht hatte ich darüber berichtet, dass der MDR verschiedene Arbeitsgruppen eingesetzt hatte, um die Datenschutzgrundverordnung umzusetzen. Da die DSGVO einen risikobasierten Ansatz verfolgt, war die Frage zu klären, wie man bei der Einführung neuer Verfahren und Systeme, die mit personenbezogenen Daten arbeiten, das Risiko betrachtet und minimiert. Aufgabe der Arbeitsgruppe war die Erarbeitung eines Handlungsleitfadens, mit Hilfe dessen die datenschutzrechtlichen Risiken eines IT-basierten Verfahrens beurteilt und die entsprechenden Maßnahmen ergriffen werden können.

Nach der Datenschutzgrundverordnung steht immer das Risiko bei der Verarbeitung der personenbezogenen Daten für die Betroffenen im Fokus. Um dieses zu minimieren, sind entsprechende geeignete technische und organisatorische Maßnahmen umzusetzen. Ein Spezialfall einer solchen Risikoabwägung ist die Datenschutz-Folgenabschätzung für den Fall, dass ein besonders hohes Risiko für die Verarbeitung personenbezogener Daten besteht. Die von der MDR-Arbeitsgruppe unter Federführung der Abteilung Informationssicherheit (Heiko Lehmann) vorgelegte Konzeption ermöglicht es den Bereichen des MDR, diese Risikoabwägung durchzuführen und eine Datenschutz-Folgenabschätzung – wenn nötig - vorzunehmen. Eckpunkte des Verfahrens sind die Prüfung der Rechtmäßigkeit der Datenverarbeitung, Bestimmung des Risikos und die daraus resultierenden notwendigen technischen und organisatorischen Maßnahmen und - bei Bestehen entsprechender Anhaltspunkte - die Prüfung und ggf. Durchführung einer Datenschutz-Folgenabschätzung. Ich gehe davon aus, dass beim MDR eine solche Folgenabschätzung nur im Ausnahmefall nötig sein wird. Aber dann ist der Handlungsleitfaden ein nützliches Instrument, um mit Unterstützung des betrieblichen Datenschutzbeauftragten ein solches Verfahren durchzuführen. Ebenso wird in dem Handlungsleitfaden erläutert, wie die Vorgaben zu privacy by design und privacy by default umzusetzen sind. Damit gemeint sind der bei Konzeption eines neuen Verfahrens vorzusehende Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Die in der Konzeption enthaltene Check-

liste erlaubt es den verantwortlichen Bereichen, hier datenschutzkonform zu agieren.

Es ist gelungen, ein sich an der Komplexität dieser Vorgaben orientiertes Handlungsgerüst für die verantwortlichen Fachbereiche des MDR zu erarbeiten. Die Datenschutzgrundverordnung erfordert eine genaue Dokumentation des beschriebenen Prozess und der daraus resultierenden Maßnahmen zur Risikominimierung. Um diesen relativ komplexen Prozess zu erleichtern, stellt der Handlungsleitfaden ein nützliches Hilfsmittel dar.

Im Berichtszeitraum war die Integration in die Prozesse und Regeln des MDR noch nicht abgeschlossen. Insoweit werde ich weiter berichten.

4.7 Umsetzung Datenschutzgrundverordnung - Löschkonzept

Im letzten Tätigkeitsbericht für den Zeitraum 01.07.2016 - 31.07.2018 habe ich darüber berichtet, dass sich eine Arbeitsgruppe bei der Umsetzung der Datenschutzgrundverordnung mit Löschkonzepten befasst hat. Ich hatte beschrieben, dass ein Konzept gefunden werden müsse, das flexibel einsetzbar ist und die beteiligten Bereiche befähigt, eigenständig über die Löschung bei ihnen vorgehaltener Daten zu entscheiden. Im September 2019 ist ein solcher Handlungsleitfaden von der Arbeitsgruppe verabschiedet worden. In dieser Arbeitsgruppe waren fast sämtliche Bereiche des MDR beteiligt, sodass ein breiter Konsens über die getroffenen Maßnahmen erzielt werden konnte. Diskutiert wurde im Rahmen der Erstellung des Konzepts insbesondere, wann eine datenschutzgerechte Löschung tatsächlich anzunehmen sei. Unter Löschung versteht man in diesem Zusammenhang die Unbrauchbarmachung bzw. Unkenntlichmachung von Daten, sodass deren Rekonstruktion nur theoretisch bzw. nur mit unverhältnismäßig hohem Aufwand möglich ist. Problematisch ist, dass sich das Löschen von Sicherungskopien bzw. Backups in diesem Zusammenhang als schwierig erweist, da ein zielgenaues Löschen einzelner Daten in diesen Speichermedien nicht möglich ist. Daher wird hier mit einem sehr strengen Berechtigungskonzept dafür gesorgt, dass eine Wiederherstellung von Daten nur in Ausnahmefällen und wenn es tatsächlich notwendig ist, durchgeführt werden darf und bereits zuvor gelöschte Daten auch wiederum nach Wiederherstellung gelöscht werden müssen. Dieses Löschkonzept

bzw. der Handlungsleitfaden zum Löschen personenbezogener Daten nach DSGVO postuliert neben der Pflicht zur Datenlöschung auch grundsätzliche Handlungsregeln zur Archivierung und Aufbewahrung im MDR. Er legt Fristen zwischen Ablauf der Aufbewahrungsfrist und der Durchführung der Löschung fest und enthält Hinweise zur Vernichtung von Datenträgern. Auch die Protokollierung von Löschungen muss gewährleistet sein. Im Übrigen wird vorgegeben, wie mit dem Recht auf Löschung nach Artikel 17 DSGVO umgegangen werden soll. Als Anlage enthält diese Handreichung eine Übersicht über ausgewählte gesetzliche Aufbewahrungsfristen. Hier liegt es in der Verantwortung der einzelnen Bereiche des MDR, die speziell zu treffenden gesetzlichen Aufbewahrungsfristen zu kennen und entsprechend umzusetzen. Insgesamt muss sich jeder Bereich eigenständig klarmachen, wie genau die Löschung umgesetzt wird. Mit dem allgemeinen Handlungsfaden hat der MDR aber ein taugliches Konzept entwickelt, um die Umsetzung dieser gesetzlichen Pflicht zu erleichtern. Eine Integration dieses Konzeptes in die Regeln des MDR war zum Ende des Berichtszeitraums noch nicht umgesetzt. Auch hierzu werde ich weiter berichten.

4.8 Neugestaltung des Verzeichnisses von Verarbeitungstätigkeiten

Gemäß Artikel 30 der Datenschutzgrundverordnung muss auch der MDR ein Verzeichnis von Verarbeitungstätigkeiten anlegen und führen. Bereits zu Beginn des Jahres 2018 – also kurz vor Geltung der Datenschutzgrundverordnung – hat der MDR in einer eigens dafür einberufenen Arbeitsgruppe große Anstrengungen unternommen, um ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Hierin sind alle Verfahren aufzuführen, in denen Daten von Personen verarbeitet werden. Hierbei kann es durchaus zu Abgrenzungsschwierigkeiten und definitorischen Unschärfen kommen, die auch bis heute nicht vollständig geklärt sind. Letztendlich muss jede verantwortliche Stelle entscheiden, wie feingranular ein solches Verzeichnis ausgestaltet wird. Nach meinem Dafürhalten, ist dies beim MDR in guter Weise gelungen, jedoch hat sich gezeigt, dass durch die vielen verschiedenen Verarbeitungstätigkeiten (insgesamt über 400), die Übersichtlichkeit gelitten hat. Dieses Verzeichnis ist nämlich dafür gedacht, der Aufsichtsbe-

hörde als erster Überblick zur Datenverarbeitung und als Nachweis für ein ordnungsgemäßes Datenschutz-Management zu dienen.

Im Zuge der Berufung der Datenschutz-Koordinatoren wurde daher beraten und überlegt, wie ein solches Verzeichnis von Verarbeitungstätigkeiten (VVT) besser und nachhaltiger gestaltet werden kann. Insbesondere die Auffindbarkeit von einzelnen Verfahren sowie ggf. vorkommende Doppelungen aufgrund der dezentralen Standorte des MDR sollten vermieden und entfernt werden.

Hier ist es gelungen, die zu benennenden Verfahren maßgeblich einzugrenzen und durch sinnvolle Zusammenfassungen tatsächlich auf unter 100 Verarbeitungstätigkeiten zu kommen.

Eine weitere Initiative des Kreises der Datenschutzkoordinatoren hat dazu geführt, eine sehr sinnvolle und aus meiner Sicht innovative Lösung voranzutreiben. Unter maßgeblicher Mitwirkung der Abteilung Informationssicherheit und des Datenschutz-Koordinators der Betriebsdirektion wird eine Datenbank aufgebaut, die eine bessere Organisation des VVT ermöglicht. So wird eine Eingabemaske erstellt, die es den einzelnen Bereichen und damit Datenschutzverantwortlichen des MDR ermöglicht, neue oder sich ändernde Verfahren in übersichtlicher Weise und vereinfacht in das VVT einzupflegen. Eine Arbeit in Excel-Tabellen oder gar Papierakten fällt damit weg und schafft neben der Übersichtlichkeit auch eine bessere Auffindbarkeit der Verfahren. Änderungen und auch Fehlerbeseitigung werden dadurch maßgeblich vereinfacht und auch der Zugriff der Datenschutz-Koordinatoren auf ein gemeinsames Verzeichnis wird dadurch ermöglicht. Zurzeit werden Anstrengungen unternommen, auch Schnittstellen zu anderen Systemen insbesondere im Rahmen von der Dokumentation und datenschutzrechtlichen Prüfung von neuen Verfahren zu etablieren. Wichtig ist hierbei, dass einmal eingepflegte Details zu Verfahren und damit vorgenommene Prüfungsschritte auch für andere datenschutzrechtliche Dokumentationen gleichfalls zur Verfügung stehen. So werden doppelte Arbeiten und etwaige Widersprüchlichkeiten von Anfang an vermieden. Dieses Projekt ist allerdings noch nicht abgeschlossen und soll im Jahre 2020 – leider aufgehalten durch die Coronakrise – abgeschlossen werden. Ich bewerte dieses Projekt und diese Initiative als äußerst positiv und könnte mir vorstellen, dass dies auch auf ARD/ZDF-Ebene Anklang finden wird.

Falls hier von der Vorarbeit des MDR profitiert werden kann, wäre dies für alle Beteiligten von Vorteil. Im Ergebnis könnte sich darauf geeinigt werden, wie die Definitionen eines Verfahrens der ARD und beim ZDF aussehen. Insofern würden die Vergleichbarkeit und damit die Zusammenarbeit zwischen den Datenschutzbeauftragten und –verantwortlichen vereinfacht. Dies ist allerdings Zukunftsmusik und muss erst noch im Arbeitskreis der Datenschutzbeauftragten beraten werden. Dazu ist selbstverständlich erforderlich, dass das Projekt beim MDR fertiggestellt wird und sich auch bewährt.

4.9 Datensicherheit - Phishing-Simulation

Datenschutz und Datensicherheit gehen Hand in Hand. Datensicherheit beschäftigt sich u.a. damit, Angriffe von außen auf die Integrität, die Vertraulichkeit und die Verfügbarkeit von Daten abzuwehren. In diesem Zusammenhang hat die Abteilung Informationssicherheit eine breit angelegte Phishing-Simulation aufgelegt, an der ich als Rundfunkdatenschutzbeauftragter beratend teilgenommen habe. Phishing bedeutet im Wesentlichen, jemanden dazu zu bringen, auf einen schädlichen Link in einer E-Mail zu klicken und private Informationen wie z. B. ein Passwort einzugeben. Dadurch können einerseits sensible Daten abfließen, andererseits besteht die Gefahr, dass durch manipulierte E-Mailanhänge Schadsoftware eingeschleust wird. Phishing stellt eine der häufigsten Formen von Cyberangriffen dar. Umso wichtiger ist es, mit Schulungen und anderen Mitteln auf dieses Problem hinzuweisen und die Aufmerksamkeit der Mitarbeiterinnen und Mitarbeiter für dieses Thema zu stärken. Dies geht am besten, wenn man mit ungefährlichen Simulationen vor Augen geführt bekommt, wie leicht man sich täuschen lässt und wie schnell man unverschuldet Opfer einer entsprechenden Attacke werden kann. Denn: Allein mit technischen Maßnahmen kann der Schutz vor solchen Angriffen nicht sichergestellt werden. Daher übernimmt jede Person, die Informationstechnik und Anwendungen nutzt, die Funktion einer „menschlichen Firewall“. Im Zuge einer Simulation mit einem ausgewählten Teilnehmerkreis wurde stichprobenhaft der aktuelle Stand des Sicherheitsverhaltens ermittelt. Mit 295 präparierten Phishing-Mails (die natürlich nicht schadenstiftend waren) wurde über einen Zeitraum von einem Monat versucht, eine Reaktion bei den teil-

nehmenden Mitarbeiterinnen und Mitarbeitern auszulösen und ihre Aufmerksamkeit dementsprechend zu erhöhen. Die gewonnenen Erkenntnisse sowie die Rückmeldungen der Teilnehmerinnen und Teilnehmer sollten eine Antwort auf die Frage geben, ob eine Ausweitung auf den gesamten MDR angezeigt ist.

Mit dieser Simulation wurde eine Firma beauftragt, mit der auch ein Auftragsverarbeitungsvertrag geschlossen worden ist. Im Zuge der teilweise sogar individualisierten Phishing-Simulation mussten natürlich auch personenbezogene Daten des MDR verarbeitet werden. Etwa wenn die Mail einen Absender aus dem Hause angibt, um damit das Vertrauen des angegriffenen Mitarbeiters zu erschleichen.

Ich selbst habe an dem Test auch teilgenommen und festgestellt, dass man ständig wachsam sein muss, um nicht auf eine solche Mail hereinzufallen. Gemeinsam mit der Abteilung Informationssicherheit konnte ein positives Fazit gezogen werden, denn die Erfahrung „am eigenen Leib" ist immens interessant, und man ist tatsächlich überrascht, wie leicht man in die Irre zu führen ist. Die Simulation hat gezeigt, dass auch die Mitarbeiterinnen und Mitarbeiter des MDR nicht vor schnellen Mausklicks auf schadhafte Inhalte gefeit sind: So wurden Phishing-Links vergleichsweise oft angeklickt und in einigen Fällen Mailanhänge ausgeführt. In der realen Welt hätte hierdurch Schadsoftware den jeweiligen Arbeitsrechner infizieren können. Manche Teilnehmerinnen und Teilnehmer gaben sogar ihre MDR-Login-Daten gegenüber einer fingierten Webseite preis (welche die Eingaben jedoch nicht annahm). In den Rückmeldungen sprach sich eine weit überwiegende Anzahl der Teilnehmenden für eine MDR-weite Phishing-Simulation aus.

Insofern unterstütze ich die Bemühungen der Abteilung Informationssicherheit ausdrücklich und auch den Plan, die Phishing-Simulation zu wiederholen und den Teilnehmerkreis deutlich auszuweiten. Die beste IT-Sicherheitsinfrastruktur nutzt nämlich nichts, wenn die Sicherheitsregeln nicht beachtet oder nur nachlässig befolgt werden. Angesichts der steigenden Bedrohungslage ist es somit notwendig, die Eigenverantwortlichkeit jedes Einzelnen zu stärken, um durch aufmerksames Verhalten die Schutzmaßnahmen der technischen Plattformen zu unterstützen. Dieses Thema wird den MDR und auch mich weiterhin beschäftigen.

5. Datenschutz beim KiKA

5.1. Zusammenarbeit mit dem KiKA

Der Kinderkanal ist eine Gemeinschaftseinrichtung von ARD und ZDF. Die betriebliche Datenschutzaufsicht obliegt der federführenden Anstalt, also dem MDR, sodass der Datenschutzbeauftragte des MDR, Herr Matthias Meincke, auch für den KiKA zuständig ist. Herr Jörn Voss, der jahrelang die datenschutzrechtlichen Belange des KiKA mitverantwortet hat, ist nach wie vor als betrieblicher Datenschutzbeauftragter des KiKA beschäftigt. Bei ihm laufen alle Fäden zusammen, er ist derjenige, der in Datenschutzfragen im KiKA angesprochen wird und dort die Entscheidungen anhand der Rechtslage zu treffen hat und ggf. Rücksprache mit Herrn Meincke und mir hält. Die Zusammenarbeit ist wie in den letzten Jahren auch problemlos und sehr kollegial. Insbesondere schnelle Kommunikationswege und fachliche Kompetenz kennzeichnen das Verhältnis. Herr Voss hat sich im Übrigen im Jahr 2019 erneut zum betrieblichen Datenschutzbeauftragten zertifizieren lassen und seine Expertise auch im Hinblick auf die DSGVO vertieft. Herr Jörn Voss erstellt jedes Jahr eine Übersicht über seine Tätigkeiten. Sein Jahresbericht 2019 ist in diesem Tätigkeitsbericht als Anlage 12.9 beigefügt.

5.2. Ene Mene Bu

Im Juni 2019 erreichte mich vom Kinderkanal eine Meldung über einen Datenschutzvorfall. Die Redaktion Vorschule des KiKA bietet eine Bildergalerie mit der Bezeichnung Ene Mene Bu an. Dort können Kinder Bilder einsenden, die von der Redaktion veröffentlicht werden. In einem Fall ist neben dem Bild der Vorname des Kindes einschließlich der vollständigen Adresse in dieser Bildergalerie veröffentlicht worden. Dies war 1,5 Tage lang der Fall, danach wurden die personenbezogenen Daten des Kindes aus dem Bild gelöscht. Dieser Vorfall ist von einem aufmerksamen Zuschauer gemeldet worden. Die Redaktion hat erläutert, dass beim Abspeichern der Datenmaske versehentlich die Adresse seitens der Redaktion nicht gelöscht worden ist. Normalerweise ist es so, dass für die Wiedererkennbarkeit des Bildes für die einreichenden Kinder der Vorname, das Alter und der Wohnort veröffentlicht werden. Ebenso anzugeben ist die E-Mail Adresse für etwaige Rückfragen, diese ist natürlich nicht zur Veröffentlichung bestimmt. Im hier

beschriebenen Fall wurde in die vorgesehene Datenmaske aber die gesamte Adresse des Kindes eingetragen. Bei der redaktionellen Bearbeitung ist dieser Umstand nicht aufgefallen, sodass es zu dieser versehentlichen Veröffentlichung der Adresse kam. Nach Erkennen des Fehlers wurde die Adresse umgehend gelöscht. Als erste Maßnahme wurde das Team erneut sensibilisiert. Der Umgang mit personenbezogenen Daten von Kindern ist besonders sorgfältig zu gestalten. Insofern muss jedes Bild, bevor es veröffentlicht wird, sehr genau überprüft werden.

Sodann stand die Frage im Raum, ob eine Benachrichtigung der betroffenen Person gemäß Artikel 34 DSGVO vorgenommen werden muss. Bei dieser Frage ist abzuwägen, ob die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen, also hier des Kindes und der Eltern, zur Folge haben könnte. Hier war zu berücksichtigen, dass das Bild nur für kurze Zeit online sichtbar war, dass ein Familienname nicht genannt wurde und eine fehlende Fotobeistellung die Identifizierbarkeit des Kindes deutlich erschwerte. Es war nicht zu erwarten, dass die Nennung der Adresse schwerwiegende Folgen für die Familie und das Kind haben würden. Unter Abwägung aller Begleitumstände war nicht anzunehmen, dass Beeinträchtigungen – wie zum Beispiel Belästigungen des Kindes oder der Familie – zu befürchten waren. Deswegen wurde entschieden, auf eine Benachrichtigung zu verzichten. Hierbei war ebenfalls zu berücksichtigen, dass eine Benachrichtigung der Familie des Kindes zu unnötiger Sorge und Aufregung hätte führen können. Daher war im Ergebnis die Entscheidung richtig, von einer Benachrichtigung abzusehen.

6. Datenschutz beim Beitragsservice

6.1 Datenschutz im Zusammenhang mit dem Rundfunkbeitrag

Der Rundfunkbeitrag wird im Privatbereich pro Wohnung erhoben wird und ist unabhängig von der Zahl der dort gemeldeten Bewohnerinnen und Bewohner und der dort befindlichen Empfangsgeräte zu entrichten. Im geschäftlichen und gewerblichen Bereich wird an die Betriebsstätten angeknüpft. Die Daten der Rundfunkbeitragszahler werden zentral in Köln durch den ARD, ZDF, Deutsch-

landradio Beitragsservice verwaltet. Spezielle Sachverhalte werden von den dezentralen Beitragsabteilungen in den einzelnen Landesrundfunkanstalten betreut. Beim MDR werden dort insbesondere die Klageverfahren abgewickelt.

Nach Maßgabe des für die einzelne Landesrundfunkanstalt geltenden Rechts sind die Datenschutzbeauftragten als Aufsicht für die Kontrolle des Zentralen Beitragsservice und der dort vorgenommenen Datenverarbeitung zuständig. Eine Ausnahme gilt insofern beim Rundfunk Berlin Brandenburg, bei Radio Bremen sowie beim Hessischen Rundfunk. Die Landesdatenschutzbeauftragten üben hier die Kontrollfunktion aus, da zwischen den Verwaltungsdaten und journalistischen Daten unterschieden wird und die Aufsicht über erstere den staatlichen Behörden obliegt. Dieses Prinzip wird unter verfassungsrechtlichem Gesichtspunkten kritisch diskutiert, da die Staatsferne des Rundfunks insoweit als beeinträchtigt angesehen wird. Die Landesdatenschutzbeauftragten agieren als staatliche Kontrollorgane, was aus grundsätzlichen Erwägungen im Hinblick auf den besonders geschützten Bereich der Rundfunkfinanzierung zumindest bedenklich ist.

Für die Daten der privaten Beitragskonten gelten die Vorschriften des Rundfunkbeitragsstaatsvertrags und ergänzend das Sächsische Datenschutzdurchführungsgesetz durch den Verweis in § 39 MDR-Staatsvertrag. Für die Kontrolle der Daten der Beitragszahler im MDR-Sendegebiet ist der Rundfunkdatenschutzbeauftragte des MDR zuständig. Beim Zentralen Beitragsservice nimmt eine behördliche Datenschutzbeauftragte die täglichen Aufgaben wahr und kümmert sich dort um die Organisation des Datenschutzes. Als Rundfunkdatenschutzbeauftragter habe ich meist dann direkt Berührung mit den Teilnehmerdaten, wenn Anfragen, Beschwerden oder auch Auskunftsersuchen von den Teilnehmerinnen und Teilnehmern direkt an mich gerichtet werden. Auskunftsersuchen werden dann zentral beim Beitragsservice in Köln bearbeitet, für sonstige Beschwerden, die die Datenverarbeitung im Rahmen des Beitragseinzugs betreffen, bin ich zuständig. Meistens werden hier beitragsrechtliche und datenschutzrechtliche Anliegen miteinander verknüpft, sodass eine enge Zusammenarbeit mit der Abteilung Beitragsservice des MDR unumgänglich ist.

Nach wie vor nimmt die Beschäftigung mit den Beitragszahler-Daten und den darum kreisenden Datenschutz einen großen Raum in den Abstimmungen im AK

DSB ein. Die Anpassungen an die Datenschutzgrundverordnung wurden beim Beitragsservice mit einem Projekt namens EUDAGO durchgeführt. Dies ist im Wesentlichen abgeschlossen. Lediglich im Hinblick auf die nicht ganz einfach zu beantwortenden Frage, wie Daten so zu löschen sind, dass die Datenverarbeitung insgesamt nicht kompromittiert wird, bedarf noch weiterer Klärungen. Hier ist eine Arbeitsgruppe beim Beitragsservice eingesetzt, die mit Hochdruck an dieser Aufgabe arbeitet. Die Datenschutzbeauftragten sind eng in diesem Prozess eingebunden und werden an den Diskussionen beteiligt.

6.2 Die Beauftragte für den Datenschutz beim Beitragsservice

Gemäß § 11 Abs. 2 Rundfunkbeitragsstaatsvertrag (RBStV) ist beim Beitragsservice in Köln ein behördlicher Datenschutzbeauftragter zu bestellen. Im Berichtszeitraum hat diese Aufgabe Frau Katharina Aye wahrgenommen. Frau Aye sorgt vor Ort für die Um- und Durchsetzung der Datenschutzregelungen und arbeitet eng mit den Mitgliedern der RDSK und des AK DSB zusammen. Die Datenschutzbeauftragte des Beitragsservice hat einen jährlichen Tätigkeitsbericht vorzulegen, der die wesentlichen datenschutzrechtlichen Fragen, die im Berichtsjahr behandelt wurden, in ausführlicher Weise beleuchtet. Frau Aye ist zudem Mitglied des AK DSB. In den Sitzungen berichtet sie regelmäßig und ausführlich über den Datenschutz beim Zentralen Beitragsservice. So konnten viele Fragen geklärt werden; zu förmlichen Beanstandungen ist es im Berichtszeitraum nicht gekommen.

6.3 Joint Controller Vereinbarung zum Zentralen Beitragsservice

Die Rundfunkanstalten verantworten gemeinsam die Datenverarbeitung durch den Zentralen Beitragsservice. Dies ist schon deshalb der Fall, weil der Zentrale Beitragsservice in Köln eine nicht rechtsfähige Verwaltungsgemeinschaft ist und insoweit keine eigene Rechtspersönlichkeit besitzt. Insoweit musste als Ergänzung zur Verwaltungsvereinbarung eine sogenannte Joint Controller Vereinbarung gemäß Artikel 26 DSGVO über die konkrete Verteilung von Verantwortlichkeiten im Rahmen des Beitragseinzuges geschlossen werden. Eine Joint Controller Vereinbarung ist ein Rechtsinstitut nach der DSGVO, das dann greift, wenn eine ein-

zelne Verantwortung für die Datenverarbeitung innerhalb eines Prozesses nicht mehr gegeben ist. Wenn gemeinsam über Mittel und Zwecke der Verarbeitung entschieden wird, so muss auch eine entsprechende Vereinbarung geschlossen werden, die festlegt, wie die Rechte und Pflichten nach der Datenschutzgrundverordnung zwischen den Verantwortlichen verteilt werden. Es geht insbesondere darum, die Wahrnehmung der Rechte der betroffenen Personen sicherzustellen und um die Übernahme der Informationspflichten gemäß der Verordnung.

Der AK DSB hat nach vielen Abstimmungsrunden eine entsprechende Vereinbarung vorgelegt, die nun seitens der entsprechenden Fachkommissionen beraten werden kann. Die finale Fassung wird dann 2020 von den Intendantinnen und Intendanten unterzeichnet werden.

In der Vereinbarung wird konkret beschrieben, um welche Verarbeitung welcher Daten es sich handelt, welche Personen betroffen sind und wer die Verantwortung für die Datenverarbeitung trägt. Dies sind hier die Landesrundfunkanstalten, das ZDF und das Deutschlandradio. Herzstück dieser Vereinbarung ist die Regelung der Pflichten nach der DSGVO. Darin ist u.a. festgelegt, dass die Betroffenenrechte in der Regel vom Beitragsservice von ARD, ZDF und Deutschlandradio für die Rundfunkanstalten bearbeitet werden und das Verzeichnis der Verarbeitungstätigkeiten im Sinne von Artikel 30 DSGVO beim Beitragsservice geführt wird. Ebenso ist hier festgelegt, wie die Meldewege gemäß Art. 33 DSGVO nach einem Datenschutzvorfall oder einer Datenschutzverletzung eingehalten werden können. Um auf eine umfassende Information des MDR bei Datenschutzverletzungen zu gewährleisten, wird neben dem Rundfunkdatenschutzbeauftragten auch die Juristische Direktion des MDR unverzüglich von dem jeweiligen Vorfall in Kenntnis gesetzt. So ist sichergestellt, dass auch der MDR als Verantwortlicher sofort und in Zusammenarbeit mit dem Rundfunkdatenschutzbeauftragten entsprechend reagieren kann.

Ebenso musste auch den Bedürfnissen des Zentralen Beitragsservice Rechnung getragen werden, nicht jede datenschutzrelevante Handlung mit den einzelnen Rundfunkanstalten individuell abstimmen zu müssen. Die Erfüllung der datenschutzrechtlichen Verpflichtungen erfolgt im Wesentlichen nach wie vor durch den Zentralen Beitragsservice.

6.4 Auskunftserteilung nach Artikel 15 DSGVO

Die Wahrnehmung des Rechtes nach Artikel 15 DSGVO auf Erteilung einer Auskunft über die erfolgte Datenverarbeitung ist das bei weitem am häufigsten beanspruchte Betroffenenrecht der DSGVO. Natürlich interessiert es viele Menschen, welche Daten von ihnen im Rahmen des Beitragseinzuges wie verarbeitet werden. Da es sich aber auch um ein Massenverfahren handelt, war auch im Rahmen des Umstellungsprozesses auf die Datenschutzgrundverordnung im Jahr 2018 sehr viel Aufwand betrieben worden, um die Auskunftserteilung einerseits vollumfänglich zu ermöglichen, andererseits aber auch dem Massenaufkommen Herr zu werden. Ende des Jahres 2018 hat sich daher eine Gruppe aus dem AK DSB gebildet, um Details bei der Auskunftserteilung zu diskutieren und ggf. zu verbessern. Im Ergebnis scheint dies gelungen, denn an den doch recht ausführlichen Auskunftserteilungen durch den Zentralen Beitragsservice gibt es kaum grundsätzliche Kritik. Im Zuge des 23. Rundfunkänderungsstaatsvertrages wird überdies der Umfang des datenschutzrechtlichen Auskunftsanspruchs beim Beitragseinzug konkretisiert und damit die Arbeit erleichtert.

7. Datenschutz bei Tochterfirmen des MDR

7.1 Datenschutzvorfall bei der Media City Atelier GmbH

Im Juli 2019 erreichte mich eine Meldung über einen Datenschutzvorfall bei der Media City Atelier (MCA) GmbH in Leipzig. Es handelte sich um die Offenlegung personenbezogener Daten durch eine automatische Weiterleitung von E-Mails an einen unbekannten Empfänger. Es geht im Wesentlichen darum, dass aus Gründen, die auch bis heute nicht ermittelt werden konnten, eine automatisierte Weiterleitung in einem E-Mail-Account einer Mitarbeiterin eingerichtet war. Diese Weiterleitung war so eingestellt, dass bei bestimmten Schlagworten wie z.B. Invoice, IBAN oder SWIFT der betreffender Text an eine Adresse unbekannten Ursprungs weitergeleitet wurden. In einer sofort einberufenen Krisensitzung habe ich mich gemeinsam mit der Geschäftsleitung der MCA darum bemüht, den Vorfall im Hinblick auf die Ursachen und die Folgen aufzuarbeiten. Dazu war zunächst notwendig zu ermitteln, wie viele Personen von dem Vorfall betroffen waren und welche Daten tatsächlich weitergeleitet worden sind. Davon hängt ab, ob

eine Benachrichtigung der betroffenen Personen durch den Verantwortlichen unverzüglich erfolgen muss. Aufgrund der (aus Gründen des Datenschutzes) nicht unbegrenzten Speicherung von E-Mail-Daten, konnten lediglich die letzten 90 Tage nach Aufdecken des Vorfalls betrachtet werden. Insgesamt hat sich gezeigt, dass ca. 130 E-Mails betroffen waren. Als Sofortmaßnahme wurde zunächst per Dienstanweisung die Einrichtung von Weiterleitungsregeln an externe Postfächer untersagt; dies muss auch regelmäßig kontrolliert werden.

Zudem ist Strafanzeige gestellt worden, jedoch konnte der Eigentümer der Zieldomain nicht ermittelt werden. Es lässt sich also nicht sagen, von welcher Seite der Angriff gestartet worden ist. Auch die gesicherte Festplatte aus dem Rechner des betroffenen E-Mail-Accounts wurde durch den betrieblichen Datenschutzbeauftragten der MCA untersucht. Der Ursprung der Weiterleitungsregel konnte jedoch auch hier nicht ermittelt werden.

Im Ergebnis sind nach Abwägungen aller Umstände sämtliche identifizierten Betroffenen mit einer ausführlichen Nachricht über den Vorfall informiert worden. Darin wurde der Vorfall detailliert beschrieben sowie die angemessene Reaktion darauf geschildert. Die Betroffenen wurden darüber informiert, dass ein Dritter möglicherweise an ihre Kontaktdaten und sonstige personenbezogenen Daten gelangt sein könnte. Die betroffenen E-Mails enthielten zwar keine sensiblen Informationen, sodass insgesamt nur von einem vergleichsweise geringen Risiko auszugehen ist, jedoch wurde den Betroffenen eine erhöhte Aufmerksamkeit bezüglich Spam-Mails und Phishing-Versuchen empfohlen - gerade dann, wenn diese Mails den Absender der MCA Leipzig angeben.

Durch die Information der Betroffenen sowie die organisatorischen Maßnahmen, die einen solchen Vorfall in Zukunft verhindern sollen, ist angemessen und richtig auf den Vorfall reagiert worden. Die Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten der MCA GmbH, Herrn Lars Nöcker, seinen Mitarbeiterinnen und Mitarbeitern sowie der Geschäftsleitung der MCA GmbH hat reibungslos geklappt und machte eine schnelle Aufklärung des Falles möglich. Ich habe deswegen und in Anbetracht des aus meiner Sicht nicht besonders hohen Risikos für die Rechte und Freiheiten der betroffenen Personen davon abgesehen, weitere aufsichtsrechtliche Maßnahmen zu ergreifen.

8. Datenschutz im IVZ

8.1 Informationsverarbeitungszentrum (IVZ)

Beim Rundfunk Berlin Brandenburg (rbb) ist die Gemeinschaftseinrichtung Informationsverarbeitungszentrum (IVZ) der ARD-Anstalten und des Deutschlandradio angesiedelt. Dort werden u.a. alle Personal- und Archivdaten für die Rundfunkanstalten verarbeitet. Auch andere Aufgaben der elektronischen Datenverarbeitung werden für die beteiligten Anstalten abgewickelt. Das IVZ unterstützt die Häuser in den Bereichen SAP, Archiv- und Produktionssysteme, IT-Support sowie Rechenzentrumsleistungen. Das IVZ wird auch die Steuerung der Vereinheitlichung der SAP-Prozesse für den gesamten öffentlichen Rundfunk übernehmen.

Ende 2018 hat das IVZ seinen Sitz vom Standort Berlin in die von dem rbb angemieteten Räumlichkeiten in Potsdam verlegt. Eine Zweigstelle ist auch beim WDR in Köln angesiedelt. Für die Kontrolle des Datenschutzes und der Datensicherheit sind alle Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Federführend ist die Datenschutzbeauftragte des rbb als Datenschutzbeauftragte der Sitzanstalt.

Einmal jährlich findet beim IVZ das „Jahrestreffen IT-Sicherheit und Datenschutz“ statt. Auf diesem Treffen informieren der Geschäftsführer und der Informationssicherheitsbeauftragte des IVZ über datenschutzrelevante Themen des zurückliegenden Jahres. Das letzte Jahrestreffen fand am 11.12.2019 per Videokonferenz statt. Schwerpunkte waren die positiven Ergebnisse des zweiten ISO 27001-Überwachungs-Audits im Oktober 2019, die geplante Verlegung des Rechenzentrums von Berlin nach Köln Bocklemünd und das Projekt (D)ein SAP. Diskutiert auch wurde die Tatsache, dass künftig wohl einige (D)ein SAP Komponenten über Clouddienste abgebildet werden müssen.

Trotz auch kontrovers diskutierter Probleme war ein aktives Eingreifen der Datenschutzbeauftragten der Anstalten nicht erforderlich.

9. Rundfunkdatenschutzkonferenz

9.1 Zusammenarbeit mit anderen Aufsichtsbehörden/Gründung der Rundfunkdatenschutzkonferenz RDSK

Durch die Neugestaltung der Rundfunkdatenschutzaufsicht musste auch die Zusammenarbeit zwischen den Datenschutzbeauftragten und den Rundfunkdatenschutzbeauftragten neu organisiert werden. Bisher sind im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) die Fäden zusammengelaufen. Dies ist eine organisatorische Struktur, die die Zusammenarbeit der Datenschutzbeauftragten der Rundfunkanstalten ermöglicht. Dieser Arbeitskreis bleibt auch weiter bestehen und berät und begleitet das operative Geschäft der Rundfunkanstalten und der Gemeinschaftseinrichtungen. Hier sind die Personen zusammengeschlossen, die als betriebliche/behördliche Datenschutzbeauftragte und Aufsichten in Anstalten oder auch Gemeinschaftseinrichtungen tätig sind.

Daneben bestand die Notwendigkeit, ein Gremium nur für die Aufsichtsbehörden zu schaffen. Deshalb wurde im April 2019 die Rundfunkdatenschutzkonferenz (RDSK) gegründet. Die Rundfunkdatenschutzkonferenz besteht aus acht Personen, die die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk über die Rundfunkanstalten ausüben. Mitglieder sind:

- Der Rundfunkdatenschutzbeauftragte des Bayerischen Rundfunkfunks, des Saarländischen Rundfunks, des Westdeutschen Rundfunks, des Deutschlandradios und des Zweiten Deutschen Fernsehens,
- der Datenschutzbeauftragte des Hessischen Rundfunks,
- der Rundfunkdatenschutzbeauftragte des Mitteldeutschen Rundfunks,
- der Rundfunkdatenschutzbeauftragte des Norddeutschen Rundfunks,
- die Datenschutzbeauftragte von Radio Bremen,
- die Datenschutzbeauftragte des Rundfunks Berlin Brandenburg,
- der Rundfunkbeauftragte für den Datenschutz beim Südwestrundfunk und
- der Datenschutzbeauftragte der Deutschen Welle.

9.2 Funktion der RDSK

Die RDSK hat sich auf eine Geschäftsordnung geeinigt. Die Aufgaben der RDSK werden wie folgt beschrieben:

Die Rundfunkdatenschutzkonferenz soll einen Beitrag zur einheitlichen Anwendung der Vorschriften der DSGVO leisten, insbesondere soweit es um die Anwendung im öffentlich-rechtlichen Rundfunk geht. Dazu arbeiten die Mitglieder in der Rundfunkdatenschutzkonferenz unter Wahrung ihrer jeweiligen Unabhängigkeit zusammen, indem sie

- sich auf die Auslegung datenschutzrechtlicher Vorschriften sowie die Ausgestaltung ihrer Zusammenarbeit verständigen (Beschluss),
- Stellung zu datenschutzpolitischen Fragen nehmen (Entschließung), und
- Orientierungshilfen, Handreichungen sowie Positionspapiere zu inhaltlichen, technischen oder organisatorischen Fragen des Datenschutzes veröffentlichen (Empfehlungen).

Die Rundfunkdatenschutzkonferenz tauscht sich unter anderem zu folgenden Themen aus:

- Aufgaben und Befugnisse gemäß Art. 57 und 58 DSGVO,
- Erstellung von Tätigkeitsberichten nach Art. 59 DSGVO,
- Kontakt zu anderen Aufsichtsbehörden gemäß Art. 51 DSGVO.

Gemäß dem in Art. 51 DSGVO verankerten Gebot der Zusammenarbeit und Kohärenz streben die Mitglieder die Zusammenarbeit mit anderen unabhängigen Datenschutz-Aufsichtsbehörden an, um ein einheitliches Datenschutzniveau zu erreichen.

9.3 Tätigkeitsschwerpunkte der RDSK

Im Jahr 2019 hat sich die RDSK zu vier Sitzungen zusammengefunden. Die fanden statt im April, im Juni, im September und im November 2019. Schwerpunkte waren, die Diskussion über die zu schaffenden organisatorischen Strukturen, auch Instrumente der Öffentlichkeitsarbeit, Vernetzung und inhaltlichen Positionierung wurden beraten. Die RDSK arbeitet unter meiner Federführung an einem

zeitgemäßen Internetauftritt, um Positionierungen, Stellungnahmen, Orientierungshilfen und den jeweiligen Stand der Datenschutzthemen dort zu veröffentlichen. Zum Vorsitzenden der RDSK wurde im Berichtszeitraum Herr Dr. Heiko Neuhoff, Rundfunkdatenschutzbeauftragter des NDR, bestimmt. Ihm oblag es, als Vorsitzender der RDSK die Termine zu koordinieren, Tagesordnungen, Sitzungen vorzubereiten und die Zusammenkünfte zu leiten. Ich war im Berichtszeitraum stellvertretender Vorsitzender der RDSK. Im Rahmen der Zusammenkünfte hat sich die RDSK schwerpunktmäßig mit folgenden Themen befasst:

- Erstellung der Geschäftsordnung der RDSK,
- Austausch über aufsichtsrechtliche Praxis, insbesondere im Hinblick auf Umgang mit Beschwerden, Aufsichtsersuchen sowie Behandlung von Datenschutzverstößen,
- Abstimmung zu Prüfungsthemen,
- Zusammenarbeit mit den staatlichen Aufsichtsbehörden,
- Aufsicht über Beteiligungsunternehmen und Gemeinschaftseinrichtungen,
- Bestellung von betrieblichen Datenschutzbeauftragten bei wichtigen Gemeinschaftseinrichtungen und Beteiligungsunternehmen,
- die EuGH-Entscheidung zu Facebook Fanpages und zur Einwilligung bei der Verwendung von Cookies,
- Fragen zur Webanalyse und dem Einsatz von First-Party-Cookies,
- Eckpunkte zum Einsatz cloudbasierter Office-Anwendungen.

Die RDSK konnte im Berichtsjahr 2019 zwei Positionspapiere fertigstellen, die sich mit dem IP-Autostart bei der Nutzung von HbbTV und dem Einsatz cloudbasierter Systeme befassen. Diese finden sich auch im Anhang zu diesem Bericht. Anfang 2020 wurde eine Empfehlung zum Einsatz von Cookies in den Online-Angeboten der Rundfunkanstalten veröffentlicht (siehe dazu auch das folgende Kapitel).

Die DSGVO sieht vor, dass die Aufsichtsbehörden miteinander ins Gespräch kommen sollen. Daher wurde der Austausch mit der Datenschutzkonferenz (DSK), das Gremium der Datenschutzaufsichtsbehörden des Bundes und der Länder verstärkt. Im Mai und Oktober 2019 wurden Einladungen des Vorsitzenden der DSK zu zwei Sitzungen zwecks Austausches der Aufsichtsbehörden der Länder, des Bundes, der Kirchen und des Rundfunks ausgesprochen. Der Bitte der RDSK um

Mitwirkung in den Arbeitskreisen der DSK wurde insoweit entsprochen, als Mitglieder der RDSK als Gäste an den Sitzungen der Arbeitskreise teilnehmen konnten. In einer Sitzung des Arbeitskreises „Grundsatzfragen“ und einer Sitzung des Arbeitskreises „technische und organisatorische Datenschutzfragen“ war daher auch die RDSK vertreten. Der intensive Austausch ist notwendig, da in der DSK und der RDSK eine Reihe von Themen mit erheblichen Überschneidungen bearbeitet wird, sodass das in Artikel 51 DSGVO niedergelegte Gebot der Zusammenarbeit und Kohärenz hier verwirklicht wird.

Die Zusammenarbeit mit anderen Aufsichtsbehörden, sei es in den Rundfunkanstalten oder mit den Behörden der Länder und des Bundes, ist unerlässlich, um die Vielzahl der Projekte mit datenschutzrechtlicher Relevanz und insbesondere die zusammenwachsenden Strukturen der ARD beratend zu überwachen.

9.4 Empfehlung zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten

Im Jahr 2019 ist im Oktober ein vielbeachtetes EuGH-Urteil ergangen. Sehr oft war zu hören, dass nach diesem Urteil der Einsatz von sogenannten Cookies auf Webseiten nur noch mit der ausdrücklichen Einwilligung der Nutzer erlaubt und damit rechtmäßig ist. Wie Pilze sprossen im Nachgang dazu die sogenannten Cookie-Banner aus dem Boden. Nach meiner Auffassung ist das ständige Auftauchen von Cookie-Bannern auch an Stellen, wo es vielleicht gar nicht unbedingt notwendig ist, der Sache des Datenschutzes eher abträglich, weil die Nutzerinnen und Nutzer den wahren Hintergrund nicht kennen und die ständigen Cookie-Banner eher als Behinderung ihres Umganges mit dem Internet wahrnehmen.

Was sind eigentlich Cookies? Ein Cookie ist eine Textdatei, die dazu dient, einzelne Rechner zu identifizieren und Anfragen miteinander zu verknüpfen. Man unterscheidet zwischen notwendigen Cookies, die für den Betrieb der Website erforderlich sind, z. B. Warenkorbfunktionen, oder Cookies, die der Sicherheit des Angebots dienen. Dann gibt es auch funktionale Cookies, die z. B. die Größe der Schriften oder die Schriftart speichern und damit Websiteinhalte individualisieren können. Andere wiederum dienen der Nutzungsmessung. Um es kurz zu machen: Notwendige und funktionale Cookies müssen nicht mit einer Einwilligung abgesi-

chert werden. Bei der Nutzungsmessung darf man nach dem Urteil des EuGH davon ausgehen, dass jeweils ein berechtigtes Interesse nachgewiesen werden muss und eine genaue Abwägung der einzelnen Umstände zu erfolgen hat. Nach Auffassung der RDSK verbreitet der öffentlich-rechtliche Rundfunk Telemedien, um seinen verfassungsrechtlichen Funktionsauftrag zu erfüllen. Er muss sein von den Beitragszahlern finanziertes Angebot auf allen publizistisch relevanten Plattformen zugänglich machen, also auch im Internet. Die Rundfunkanstalten sind dazu auf Erkenntnisse zur Akzeptanz und Nutzung ihrer Angebote angewiesen. Dies gilt nach Auffassung der RDSK jedenfalls für anonymisierte Auswertungen und damit haben die Rundfunkanstalten im Rahmen ihres verfassungsrechtlichen Funktionsauftrages ein Interesse am Einsatz von Cookies, mit denen sie die Messung ihrer Angebote sicherstellen. Mit anderen Worten: Die Nutzungsmessung gehört auch zum Auftrag des öffentlich-rechtlichen Rundfunks, sodass eine Einwilligung in diese Cookies demnach nicht erforderlich ist. Damit sind die ständigen Cookie-Banner zumindest bei den Angeboten des öffentlich-rechtlichen Rundfunkfunks im Allgemeinen nicht notwendig und finden daher auch nicht statt. Dies führt zu einem besseren Nutzungserlebnis, das jedoch nicht auf Kosten eines korrekten Datenschutzes geht.

Die RDSK hat diesbezüglich ein Empfehlungspapier für die Rundfunkanstalten erstellt, das Anfang des Jahres 2020 fertiggestellt werden konnte und sich im Anhang dieses Berichtes findet.

9.5 Projekt Dein SAP/SAP-Harmonisierung

Das ARD-weite SAP-Harmonisierungsprojekt hat zum Ziel, die Abläufe in IT-gestützten betriebswirtschaftlichen Geschäftsprozessen zu vereinheitlichen. Dies betrifft insbesondere die Finanzverwaltung, das Controlling, das Personalwesen, das Einkaufs- und Vertragswesen. Auch Abläufe der Honorarbearbeitung sowie Rechte und Lizenzen sollen über einen Zeitraum von zehn Jahren angeglichen werden. Ebenso spielen personenbezogene Daten eine wichtige Rolle, deswegen müssen die Prozesse so gestaltet werden, dass den datenschutzrechtlichen Anforderungen Genüge getan wird. Datenschutzrechtliche Vorgaben sind insofern von Anfang an zu berücksichtigen.

Auch seitens der Rundfunkdatenschutzbeauftragten ist ein Diskussionspapier erstellt worden, das die wesentlichen datenschutzrechtlichen Anforderungen formuliert, damit diesen Rechnung getragen werden kann. Hierzu gehören zunächst vertragliche Erfordernisse wie z. B.:

- Regelungen für die eingeschränkte Verarbeitung von Daten (gesperrte Daten), damit die Daten nur von einem klar definierten Personenkreis verarbeitet werden dürfen.
- Regelungen zum Verbot der Profilbildung und damit auch das Gebot, Auswertungen nur statistisch/anonym durchzuführen.
- Eine Datenverarbeitung sollte innerhalb der EU stattfinden. Eine Übermittelung darüber hinaus kann nur unter Berücksichtigung der Artikel 40 ff. DSGVO erfolgen.
- Es ist sicherzustellen, dass sensible Daten (z. B. Personaldaten) im Geltungsbereich der DSGVO verarbeitet werden. Dies auch im Hinblick darauf, dass zu erwarten ist, dass das sogenannte „Privacy Shield“ vom Europäischen Gerichtshof aufgehoben wird.
- Es ist zu gewährleisten, dass Auftragsverarbeitungsverträge den Anforderungen des Artikel 28 DSGVO genügen und das Vertragsmuster der öffentlich-rechtlichen Rundfunkanstalten verwendet wird.
- Es ist die ausdrückliche Gewährleistung von Betroffenenrechte und Kontrollrechten der Rundfunkdatenschutzbeauftragten festzuschreiben.
- Auch die Gewährleistung der Rückholbarkeit von Daten aus einer Cloud ist unabdingbar.

Weitere Anforderungen, um datenschutzrechtliche Vorgaben sicherzustellen sind u.a.:

- Eine Klassifizierung der Daten hat zu erfolgen, da davon die Anforderungen an die konkrete Verarbeitung abhängen, insbesondere der Schutzbedarf und die daraus resultierenden technischen und organisatorischen Maßnahmen. Es sind Möglichkeiten zur Löschung von Daten vorzusehen, die den gesetzlichen Anforderungen in jeder Hinsicht genügen.

- Berechtigungskonzepte müssen implementiert werden. Es sind Prozesse einzurichten, die die Datensicherheit stets auf den aktuellen Stand der Technik halten.
- Es sind - sofern vorhanden - zertifizierte Produkte einzusetzen.
- Die Einhaltung aller Vorgaben ist entsprechend Artikel 5 Abs. 2 DSGVO zu dokumentieren und nachzuweisen.

Dieses Diskussionspapier stellt die groben Mindestanforderungen an dieses Projekt aus datenschutzrechtlicher Hinsicht dar. Die Projektleitung des MDR wurde entsprechend informiert. Alle beteiligten Anstalten arbeiten eng zusammen, und dies gilt auch für die Datenschutzbeauftragten. Die Rundfunkdatenschutzbeauftragen sehen sich in der Pflicht, hier stets mit Hinweisen und Empfehlungen mitzuwirken.

10. Zusammenarbeit im Arbeitskreis der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio (AK DSB)

Der AK DSB hat sich als Gremium der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten über die letzten Jahre als Forum des Austausches und der gegenseitigen Informationen bewährt. Die von mir sehr geschätzte Zusammenarbeit mit den Kolleginnen und Kollegen wird auch weiterhin fortgesetzt werden. Dennoch hat sich Anfang des Jahres 2019 gezeigt, dass die Frage der Ausrichtung dieses Gremiums und seines Verhältnisses zur RDSK diskutiert werden musste. Im Ergebnis ist es dabei geblieben, dass der AK DSB als Gremium für alle Datenschutzbeauftragten – seien es betriebliche/behördliche oder Aufsichten – beibehalten bleibt. Insofern sind die Themen nach wie vor vielfältig und die Schnittmenge zwischen betrieblichen Datenschutz und Aufsichten werden in diesem Gremium erschöpfend besprochen.

Schwerpunktmäßig hat sich der AK DSB im Berichtszeitraum mit folgenden Themen befasst:

- Entwurf des 23. Rundfunkänderungsstaatsvertrages (RÄStV),
- Entwurf einer Vereinbarung zur gemeinsamen Verantwortung beim Beitragsservice (Joint Controller Vereinbarung),
- Schwärzung auf Kopien von Leistungsbescheiden zwecks Befreiung von der Rundfunkbeitragspflicht,
- Umsetzung der DSGVO beim Beitragsservice im Zusammenhang mit dem Löschkonzept,
- Aktueller und zukünftiger Umgang mit Datenschutzverletzungen beim ZBS,
- Entwicklungen der Datenschutzgesetzgebung und –politik
- Datenschutzrechtliche Begleitung der SAP Harmonisierung,
- Akkreditierung bei der DFL–Datenerhebung durch Sportcast,
- Umsetzung der Datenschutzgrundverordnung und Vereinheitlichung der Datenschutz-Folgenabschätzung sowie Risikoanalyse in den Häusern,
- Office 365,
- Überarbeitung des Musters zur Auftragsverarbeitung,
- Zentrales SIEM/SOC für die ARD,
- E-Learning Angebote der Medienakademie zum Datenschutz,
- Anpassung sonstiger Verträge, insbesondere Auftragsproduktionsverträge an die datenschutzrechtlichen Anforderungen,
- Erstellung eines Cloud-Guides;
- Vorgehen in Sachen EuGH-Urteil zu Facebook Fanpages und „Gefällt mir-Button“,
- Datenschutz beim IVZ,
- Datenschutz und Datensicherheit für die journalistische Arbeit.

Im Berichtszeitraum war Herr Dr. Heiko Neuhoff Vorsitzender des AK DSB und als solcher verantwortlich für die Erstellung der Tagesordnung, der Einberufung der Sitzungen sowie die Leitungen der Zusammenkünfte. Herr Dr. Neuhoff hat sich in hervorragender Weise für die Sache des AK DSB und auch der RDSK engagiert. Seine Stellvertretung habe ich übernommen.

11. Schlussbemerkungen

Das Jahr 2019 war in organisatorischer Hinsicht insbesondere geprägt durch die Gründung der Rundfunkdatenschutzkonferenz (RDSK) als Gremium der Rundfunkdatenschutzbeauftragten und datenschutzrechtlichen Aufsichten über die öffentlich-rechtlichen Rundfunkanstalten. Dies hat etliche Neuerungen gebracht und erforderte sowohl inhaltlichen sowohl als auch organisatorischen Aufwand.

Nicht zuletzt wegweisende Entscheidungen der höchsten Gerichte haben direkte Auswirkungen auch auf die Arbeit der Rundfunkanstalten. So wird immer wieder die Frage neu gestellt werden müssen, unter welchen Voraussetzungen Nutzungsmessung im Online-Bereich möglich ist und in welcher Form eine Präsenz des MDR in den Sozialen Netzwerken auch aus datenschutzrechtlicher Sicht als unbedenklich bezeichnet werden kann.

Ich habe die Hoffnung, dass dieser Bericht einen Einblick in meine Tätigkeit als Rundfunkdatenschutzbeauftragter beim MDR ermöglicht. Die Tätigkeit im Bereich des Datenschutzes hat mir viel Freude gemacht. Dafür darf ich mich ausdrücklich bei den Gremien des MDR für das in mich gesetzte Vertrauen und der Geschäftsleitung und allen Mitarbeiterinnen und Mitarbeitern des MDR für die vertrauensvolle Zusammenarbeit bedanken.

12. Anhang

Gesetzliche Grundlagen

12.1 MDR-Staatsvertrag (§§ 39 bis 42)

§ 39 Geltung von Datenschutzvorschriften

Soweit nachfolgend nichts anderes bestimmt ist, sind für den MDR die Vorschriften des Freistaates Sachsen über den Schutz personenbezogener Daten anzuwenden.

§ 40 Datenverarbeitung zu journalistischen Zwecken, Medienprivileg

(1) Soweit der MDR personenbezogene Daten zu journalistischen Zwecken verarbeitet, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen Zwecken von der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz der natürlichen Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119/1 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) außer den Kapiteln I, VIII, X und XI nur die Artikel 5 Absatz 1 lit. f in Verbindung mit Absatz 2, Artikel 24 und 32 Anwendung. Artikel 82 und 83 der Verordnung (EU) 2016/679 gelten mit der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses gemäß der Sätze 1 bis 3 sowie für unzureichende Maßnahmen nach Artikel 5 Absatz 1 lit. f, Artikel 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird. Die Sätze 1 bis 5 gelten entsprechend für die zu den in Satz 1 genannten Stellen gehörenden Hilfs- und Beteiligungsunternehmen. Der MDR kann sich einen Verhaltenskodex geben, der in einem transparenten Verfahren erlassen und veröffentlicht wird. Den betroffenen Personen stehen nur die in den Absätzen 2 und 3 genannten Rechte zu.

(2) Führt die journalistische Verarbeitung personenbezogener Daten zur

Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, so sind diese Gegendarstellungen, Verpflichtungserklärungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

(3) Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, kann die betroffene Person Auskunft über die der Berichterstattung zu Grunde liegenden zu ihrer Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde.
4. Die betroffene Person kann die unverzügliche Berichtigung unrichtiger personenbezogener Daten im Datensatz oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Die weitere Speicherung der personenbezogenen Daten ist rechtmäßig, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Wahrnehmung berechtigter Interessen erforderlich ist.

§ 41 Rechte der Betroffenen

(wurde aufgehoben)

§ 42 Ernennung des Rundfunkbeauftragten für den Datenschutz beim MDR und des Datenschutzbeauftragten des MDR

(1) Der MDR ernennt einen Rundfunkbeauftragten für den Datenschutz beim MDR (Rundfunkdatenschutzbeauftragter), der zuständige Aufsichtsbehörde im Sinne des Artikels 51 der Verordnung (EU) 2016/679 ist. Die Ernennung erfolgt durch den Rundfunkrat mit Zustimmung des Verwaltungsrates für die Dauer von vier Jahren. Eine dreimalige Wiederernennung ist zulässig. Der Rundfunkdatenschutzbeauftragte muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, nachgewiesen durch ein abgeschlossenes Hochschulstudium, sowie über Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Das Amt des Rundfunkdatenschutzbeauftragten kann nicht neben anderen Aufgaben innerhalb des MDR und seiner Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt des Rundfunkdatenschutzbeauftragten zu vereinbaren sein und dürfen seine Unabhängigkeit nicht gefährden.

(2) Das Amt endet mit Ablauf der Amtszeit, mit Rücktritt vom Amt oder mit Erreichen des gesetzlichen Renteneintrittsalters. Tarifvertragliche Regelungen bleiben unberührt. Der Rundfunkdatenschutzbeauftragte kann seines Amtes nur enthoben werden, wenn er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt. Dies geschieht durch Beschluss des Rundfunkrates auf Vorschlag des Verwaltungsrates; der Rundfunkdatenschutzbeauftragte ist vor der Entscheidung zu hören.

(3) Das Nähere, insbesondere die Grundsätze der Vergütung, beschließt der Rundfunkrat mit Zustimmung des Verwaltungsrates in einer Satzung.

(4) Der Datenschutzbeauftragte des MDR gemäß Artikel 37 der Verordnung (EU) 2016/679 wird vom Intendanten mit Zustimmung des Verwaltungsrates benannt.

§ 42 a Unabhängigkeit des Rundfunkdatenschutzbeauftragten

(1) Der Rundfunkdatenschutzbeauftragte ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er unterliegt keiner Rechts- oder Fachaufsicht. Der Dienstaufsicht des Verwaltungsrates untersteht er nur insoweit, als seine Unabhängigkeit bei der Ausübung seines Amtes dadurch nicht beeinträchtigt wird.

(2) Die Dienststelle des Rundfunkdatenschutzbeauftragten wird bei der Geschäftsstelle von Rundfunkrat und Verwaltungsrat eingerichtet. Dem Rundfunkdatenschutzbeauftragten ist die für die Erfüllung seiner Aufgaben und Befugnisse notwendige Personal-, Finanz- und Sachausstattung zur Verfügung zu stellen. Die erforderlichen Mittel sind jährlich, öffentlich und gesondert im Haushaltsplan des MDR auszuweisen und dem Rundfunkdatenschutzbeauftragten im Haushaltsvollzug zuzuweisen. Einer Finanzkontrolle durch den Verwaltungsrat unterliegt der Rundfunkdatenschutzbeauftragte nur insoweit, als seine Unabhängigkeit bei der Ausübung seines Amtes dadurch nicht beeinträchtigt wird.

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

§ 42 b Aufgaben und Befugnisse des Rundfunkdatenschutzbeauftragten

(1) Der Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Datenschutzvorschriften dieses Staatsvertrages, des Rundfunkstaatsvertrages, der Verordnung (EU) 2016/679 und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des MDR und seiner Beteiligungsunternehmen im Sinne des § 16c Absatz 3 Satz 1 des Rundfunkstaatsvertrages. Er hat die Aufgaben und Befugnisse entsprechend der Artikel 57 und Artikel 58 Absatz 1 bis 5 der Verordnung (EU) 2016/679. Bei der Zusammenarbeit mit anderen Aufsichtsbehörden hat er, soweit die Datenverarbeitung zu journalistischen Zwecken betroffen ist, den Schutz von Informanten zu wahren. Er kann gegenüber dem MDR keine Geldbußen verhängen.

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

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

(4) Der Rundfunkdatenschutzbeauftragte erstattet jährlich auch den Organen des MDR den schriftlichen Bericht im Sinne von Artikel 59 der Verordnung (EU) 2016/679 über seine Tätigkeit. Der Bericht wird veröffentlicht, wobei eine Veröffentlichung im Online-Angebot des MDR ausreichend ist.

(5) Jedermann hat das Recht, sich unmittelbar an den Rundfunkdatenschutzbeauftragten zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch das MDR oder seiner Beteiligungsunternehmen im Sinne des Absatzes 1 Satz 1 in seinen schutzwürdigen Belangen verletzt zu sein.

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

12.2 MDR-Datenschutzsatzung

Satzung über die Rundfunkbeauftragte für den Datenschutz beim MDR (Rundfunkdatenschutzbeauftragte)

In Ausführung des § 42 Abs. 3 MDR-Staatsvertrag hat der Rundfunkrat mit Beschluss vom 18.06.2018 und mit Zustimmung des Verwaltungsrats vom 18.06.2018 die nachstehende Satzung erlassen:

I. Stellung und Aufgaben der Rundfunkdatenschutzbeauftragten

Art. 1 – Stellung der Rundfunkdatenschutzbeauftragten

(1) Die Rundfunkdatenschutzbeauftragte beim MDR ist eine vom Mitteldeutschen Rundfunk und seinen Organen unabhängige Aufsichtsbehörde im Sinne des Art. 51 der Verordnung (EU) 2016/679 (DSGVO).

(2) Die Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Vorschriften über den Datenschutz, insbesondere der DSGVO sowie gemäß § 39 MDR-StV die Vorschriften des Freistaates Sachsen über den Schutz personenbezogener Daten im Mitteldeutschen Rundfunk und seinen Hilfs- und Beteiligungsunternehmen. Sie leistet einen Beitrag zur einheitlichen Anwendung der DSGVO in der gesamten Europäischen Union und bei den öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland.

Art. 2 - Aufgaben und Befugnisse der Rundfunkdatenschutzbeauftragten

(1) Die Rundfunkdatenschutzbeauftragte nimmt die ihr nach § 42b MDR-StV in Verbindung mit Art. 57 DSGVO obliegenden Aufgaben wahr. Zur Durchführung der Aufgaben verfügt sie über die in § 42b MDR-StV und Art. 58 Absätze 1 bis 5 DSGVO vorgesehenen Befugnisse.

(2) Gebühren nach Art. 57 Absatz 4 DSGVO bemessen sich nach dem Justizvergütungs- und Entschädigungsgesetz (JVEG) in seiner jeweils geltenden Fassung.

(3) Für den Fall ihrer Verhinderung über einen Zeitraum von länger als zwei Monaten bestimmt die Rundfunkdatenschutzbeauftragte eine Vertreterin.

(4) Die Dienststelle als Behördensitz der Rundfunkdatenschutzbeauftragten lautet:
Mitteldeutscher Rundfunk
Kantstraße 71–73
04275 Leipzig

II. Vergütung und Ausstattung der Rundfunkdatenschutzbeauftragten

Art. 3 – Grundsätze der Vergütung und Ausstattung

(1) Die Festlegung der Vergütung erfolgt durch den Verwaltungsrat für die Dauer der Amtszeit der Rundfunkdatenschutzbeauftragten.
(2) Bei der Festlegung der Vergütung sind insbesondere die berufliche Erfahrung, fachliche Qualifikation und persönliche Eignung der Rundfunkdatenschutzbeauftragten zu berücksichtigen.
(3) Der Verwaltungsrat genehmigt den Bedarf für die Personal-, Finanz- und Sachausstattung der Rundfunkdatenschutzbeauftragten und übt die Finanzkontrolle unter Berücksichtigung der Unabhängigkeit des Amtes aus. Dabei muss stets sichergestellt werden, dass die Personal-, Finanz- und Sachausstattung den Anforderungen des Art. 52 Abs. 4 DSGVO entspricht.

III. Kooperation bei der Datenschutzaufsicht mit anderen öffentlich-rechtlichen Rundfunkanstalten

Art. 4 - Möglichkeit der mehrfachen, koordinierten Ernennung derselben Person

Der Rundfunkrat kann mit Zustimmung des Verwaltungsrats zur Rundfunkdatenschutzbeauftragten eine Person ernennen, die gleichzeitig das Amt nach Art. 51 DSGVO für eine oder mehrere weitere öffentlich-rechtliche Rundfunkanstalt/-en ausübt. Eine derartige Tätigkeit ist mit dem Amt der Rundfunkdatenschutzbeauftragten vereinbar im Sinne des § 42 Absatz 1 Satz 5 MDR-StV.

Art. 5 - Ausübung des Amts bei mehrfacher Ernennung

(1) Sofern und solange die Rundfunkdatenschutzbeauftragte nach Artikel 4 dieser Satzung zum Mitglied der Datenschutzaufsichtsbehörde nach Art. 51 DSGVO für mindestens eine weitere öffentlich-rechtliche Rundfunkan-

stalt ernannt ist oder wird, gelten der nachfolgende Absatz 2 sowie die nachfolgenden Artikel 6 und 7.

(2) Stellung und Aufgaben gemäß Artikel 1 und 2 dieser Satzung bleiben von der gleichzeitigen Ernennung durch eine andere Rundfunkanstalt im Grundsatz unberührt.

Art.6 - Grundsätze der Vergütung und Ausstattung bei mehrfacher Ernennung

(1) Bei der Festlegung der Vergütung im Rahmen einer gleichzeitigen Ernennung nach diesem Abschnitt III. ist ergänzend zu Artikel 3 dieser Satzung zudem das Maß an Verantwortung zu berücksichtigen, das insbesondere in der Anzahl der beteiligten Anstalten zum Ausdruck kommt.

(2) Der Verwaltungsrat genehmigt den Bedarf für die Personal-, Finanz- und Sachausstattung der Rundfunkdatenschutzbeauftragten im Rahmen einer gleichzeitigen Ernennung nach diesem Abschnitt III. ergänzend zu Artikel 3 dieser Satzung unter Berücksichtigung von Beiträgen der anderen beteiligten öffentlich-rechtlichen Rundfunkanstalt/-en zur Ausstattung.

(3) Das Nähere, insbesondere die jeweiligen Anteile am Finanzierungsaufwand sowie die für die Sicherstellung der Finanzkontrolle notwendigen und dementsprechend einzuräumenden Informationsrechte und -pflichten zwischen den beteiligten öffentlich-rechtlichen Rundfunkanstalten, kann der Mitteldeutsche Rundfunk mit der/den beteiligten öffentlich-rechtlichen Rundfunkanstalt/-en durch Verwaltungsvereinbarung regeln. Die Anforderungen des Artikel 3 Absatz 3 Satz 2 dieser Satzung bleiben unberührt.

Art. 7 - Dienstaufsicht bei mehrfacher Ernennung oder Dienstverhältnis mit anderer Rundfunkanstalt

(1) Sofern ein Dienstverhältnis zwischen der das Amt der Rundfunkdatenschutzbeauftragten ausübenden Person und dem Mitteldeutschen Rundfunk besteht, übt der Verwaltungsrat eine eingeschränkte Dienstaufsicht insoweit aus, als die Unabhängigkeit der Rundfunkdatenschutzbeauftragten bei der Ausübung des Amtes dadurch nicht beeinträchtigt wird. Über geplante und

ausgeführte Dienstaufsichtsmaßnahmen, die andere nach diesem Abschnitt III. beteiligte öffentlich-rechtliche Rundfunkanstalt/-en betreffen, mit der kein Dienstverhältnis besteht, informiert der Verwaltungsrat die gesetzlich für die Dienstaufsicht zuständigen Gremien der entsprechenden Anstalt/-en.

(2) Soweit die das Amt der Rundfunkdatenschutzbeauftragten ausübende Person in einem Dienstverhältnis zu einer anderen öffentlich-rechtlichen Rundfunkanstalt steht, ist sicherzustellen, dass im Rahmen dieses Dienstverhältnisses die Unabhängigkeit der Rundfunkdatenschutzbeauftragten und die Kompetenzen des Rundfunk- und Verwaltungsrates des Mitteldeutschen Rundfunks gewahrt bleiben. Vorzusehen sind dabei insbesondere Verpflichtungen der die Dienstaufsicht führenden öffentlich-rechtlichen Rundfunkanstalt entsprechend des Absatzes 1 dieses Artikels. Das Nähere kann der Mitteldeutsche Rundfunk mit der/den beteiligten öffentlich-rechtlichen Rundfunkanstalt/-en durch Verwaltungsvereinbarung regeln.

IV. Schlussbestimmungen

Art. 8 - Satzungsänderung

(1) Die Satzung kann durch Beschluss des Rundfunkrats mit zwei Dritteln der Stimmen aller anwesenden Mitglieder geändert werden.

(2) Will der Rundfunkrat die Satzung ändern, hat er vorher den Verwaltungsrat zu hören.

(3) Der Verwaltungsrat kann Änderungen der Satzung vorschlagen.

Art. 9 - Inkrafttreten und Bekanntgabe

(1) Diese Satzung tritt am 19.06.2018 in Kraft.

(2) Sie wird in den amtlichen Mitteilungsblättern der Länder Sachsen, Sachsen-Anhalt und Thüringen bekanntgegeben

12.3 Artikel 85 EU-Datenschutz-Grundverordnung (DSGVO)

Art. 85 Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

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

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

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

12.4 Rundfunkbeitragsstaatsvertrag (§§ 11 und 14)

§ 11 Verwendung personenbezogener Daten

(1) Beauftragt die Landesrundfunkanstalt Dritte mit Tätigkeiten bei der Durchführung des Beitragseinzugs oder der Ermittlung von Beitragsschuldnern, die der Anzeigepflicht nach § 8 Abs. 1 nicht oder nicht vollständig nachgekommen sind, so gelten für die Erhebung, Verarbeitung und Nutzung der dafür erforderlichen Daten die für die Datenverarbeitung im Auftrag anwendbaren Bestimmungen.

(2) Beauftragen die Landesrundfunkanstalten eine Stelle nach § 10 Abs. 7 Satz 1 mit Tätigkeiten bei der Durchführung des Beitragseinzugs und der Ermittlung von Beitragsschuldnern, ist dort unbeschadet der Zuständigkeit des nach Landesrecht für die Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ein behördlicher Datenschutzbeauftragter zu bestellen. Er arbeitet zur Gewährleistung des Datenschutzes mit dem nach Landesrecht für die Landesrundfunkanstalt zuständigen Datenschutzbeauftragten zusammen und unterrichtet diesen über Verstöße gegen Datenschutzvorschriften sowie die dagegen getroffenen Maßnahmen. Im Übrigen gelten die für den behördlichen Datenschutzbeauftragten anwendbaren Bestimmungen des Bundesdatenschutzgesetzes entsprechend.

(3) Die zuständige Landesrundfunkanstalt darf von ihr gespeicherte personenbezogene Daten der Beitragsschuldner an andere Landesrundfunkanstalten auch im Rahmen eines automatisierten Abrufverfahrens übermitteln, soweit dies zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden oder der empfangenden Landesrundfunkanstalt beim Beitragseinzug erforderlich ist. Es ist aufzuzeichnen, an welche Stellen, wann und aus welchem Grund welche personenbezogenen Daten übermittelt worden sind.

(4) Die zuständige Landesrundfunkanstalt kann für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach diesem Staatsvertrag besteht, personenbezogene Daten bei öffentlichen und nicht öffentlichen Stellen ohne Kenntnis des Betroffenen erheben, verarbeiten oder nutzen. Öffentliche Stellen im Sinne von Satz 1 sind solche, die zur Übermittlung der Daten einzelner Inhaber von Wohnungen oder Betriebsstätten befugt sind. Dies sind insbesondere Meldebehörden, Handelsregister, Gewerberegister und Grundbuchämter. Nicht-

öffentliche Stellen im Sinne von Satz 1 sind Unternehmen des Adresshandels und der Adressverifizierung. Voraussetzung für die Erhebung der Daten nach Satz 1 ist, dass

1. eine vorherige Datenerhebung unmittelbar beim Betroffenen erfolglos war oder nicht möglich ist,

2. die Datenbestände dazu geeignet sind, Rückschlüsse auf die Beitragspflicht zuzulassen, ins- besondere durch Abgleich mit dem Bestand der bei den Landesrundfunkanstalten gemeldeten Beitragsschuldner, und

3. sich die Daten auf Angaben beschränken, die der Anzeigepflicht nach § 8 unterliegen und kein erkennbarer Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat.

Die Erhebung, Verarbeitung oder Nutzung bei den Meldebehörden beschränkt sich auf die in § 14 Abs. 9 Nr. 1 bis 8 genannten Daten. Daten, die Rückschlüsse auf tatsächliche oder persönliche Verhältnisse liefern könnten, dürfen nicht an die übermittelnde Stelle rückübermittelt werden. Das Verfahren der regelmäßigen Datenübermittlung durch die Meldebehörden nach dem Bundesmeldegesetz oder den Meldedatenübermittlungsverordnungen der Länder bleibt unberührt. Die Daten Betroffener, für die eine Auskunftssperre gemäß § 51 des Bundesmeldegesetzes gespeichert ist, dürfen nicht übermittelt werden.

(5) Im nicht privaten Bereich darf die zuständige Landesrundfunkanstalt Telefonnummern und E-Mail- Adressen bei den in Absatz 4 Satz 1 genannten Stellen und aus öffentlich zugänglichen Quellen ohne Kenntnis des Betroffenen erheben, verarbeiten und nutzen, um Grund und Höhe der Beitragspflicht festzustellen.

(6) Die Landesrundfunkanstalt darf die in den Absätzen 4 und 5 und in § 4 Abs. 7, § 8 Abs. 4 und 5 und § 9 Abs. 1 genannten Daten und sonstige freiwillig übermittelte Daten nur für die Erfüllung der ihr nach diesem Staatsvertrag obliegenden Aufgaben erheben, verarbeiten oder nutzen. Die erhobenen Daten sind unverzüglich zu löschen, wenn feststeht, dass sie nicht mehr benötigt werden oder eine Beitragspflicht dem Grunde nach nicht besteht. Nicht überprüfte Daten

sind spätestens nach zwölf Monaten zu löschen. Jeder Beitragsschuldner erhält eine Anmeldebestätigung mit den für die Beitragserhebung erforderlichen Daten.

(7) Auf das datenschutzrechtliche Auskunftsersuchen eines Beitragsschuldners hat die zuständige Landesrundfunkanstalt dem Beitragsschuldner die Stelle mitzuteilen, die ihr die jeweiligen Daten des Beitragsschuldners übermittelt hat.

§ 14 Übergangsbestimmungen

(9) Um einen einmaligen Abgleich zum Zwecke der Bestands- und Ersterfassung zu ermöglichen, übermittelt jede Meldebehörde für einen bundesweit einheitlichen Stichtag automatisiert innerhalb von längstens zwei Jahren ab dem Inkrafttreten dieses Staatsvertrages gegen Kostenerstattung einmalig in standardisierter Form die nachfolgenden Daten aller volljährigen Personen an die jeweils zuständige Landesrundfunkanstalt:

1. Familienname,
2. Vornamen unter Bezeichnung des Rufnamens,
3. frühere Namen,
4. Doktorgrad,
5. Familienstand,
6. Tag der Geburt,
7. gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen, einschließlich aller vorhandenen Angaben zur Lage der Wohnung und
8. Tag des Einzugs in die Wohnung.

Hat die zuständige Landesrundfunkanstalt nach dem Abgleich für eine Wohnung einen Beitragsschuldner festgestellt, hat sie die Daten der übrigen dort wohnenden Personen unverzüglich zu löschen, sobald das Beitragskonto ausgeglichen ist. Im Übrigen darf sie die Daten zur Feststellung eines Beitragsschuldners für eine Wohnung nutzen, für die bislang kein Beitragsschuldner festgestellt wurde; Satz 2 gilt entsprechend. Die Landesrundfunkanstalt darf die Daten auch zur Aktualisierung oder Ergänzung von bereits vorhandenen Teilnehmerdaten nutzen. § 11 Abs. 6 Satz 2 und 3 gilt entsprechend.

(9a) Zur Sicherstellung der Aktualität des Datenbestandes wird zum 1. Januar 2018 ein weiterer Abgleich entsprechend Absatz 9 durchgeführt. Die Meldebehörden übermitteln die Daten bis längstens 31. Dezember 2018. Im Übrigen gelten Absatz 9 Satz 1 bis 4 und § 11 Abs. 6 Satz 2 und 3 entsprechend. Der Abgleich wird nach seiner Durchführung evaluiert. Die Landesrundfunkanstalten stellen den Ländern hierfür die erforderlichen Informationen zur Verfügung.

12.5 MDR-Rundfunkbeitragssatzung (§§ 7 bis 9)

§ 7 Datenerhebung bei öffentlichen Stellen

(1) Die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle wird eine andere öffentliche Stelle um die Übermittlung personenbezogener Daten gemäß § 11 Abs. 4 RBStV nur ersuchen, soweit eine vorherige Datenerhebung unmittelbar beim Betroffenen erfolglos war oder nicht möglich ist. Dabei werden nur die in § 8 Abs. 4 und 5 RBStV genannten Daten unter den Voraussetzungen von § 11 Abs. 4 Satz 5 RBStV erhoben. Die Verfahren der regelmäßigen Datenübermittlung durch die Meldebehörden nach den entsprechenden Regelungen der Länder und der Meldedatenübermittlung nach § 14 Abs. 9 und 9a RBStV bleiben unberührt.

(2) Die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle wird personenbezogene Daten nach Absatz 1 bei öffentlichen Stellen nur erheben, um

1. bisher unbekannte Beitragsschuldner festzustellen oder
2. die von ihr gespeicherten Daten von Beitragsschuldnern im Rahmen des Datenkatalogs nach § 8 Abs. 4 und 5 RBStV zu berichtigen, zu ergänzen oder zu löschen.

§ 8 Datenerhebung bei nichtöffentlichen Stellen

(1) Die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle darf ein Auskunftsverlangen an die in § 9 Abs. 1 Satz 2 und 3 RBStV genannten Personen nur richten, wenn ein vorheriges Auskunftsverlangen unmittelbar beim Betroffenen nach § 9 Abs. 1 Satz 1 RBStV und eine Anfrage bei der Meldebehörde oder dem maßgeblichen öffentlichen Register nach § 11 Abs. 4 Satz 2 und 3

RBStV erfolglos geblieben ist oder nicht möglich war. Die Auskunft ist schriftlich zu erteilen und auf die Daten nach § 8 Abs. 4 Nr. 3 RBStV der jeweiligen Inhaber der betreffenden Wohnung oder Betriebsstätte beschränkt.

(2) Vorbehaltlich der Regelungen in Absatz 1 darf die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle als nichtöffentliche Stelle nur Unternehmen des Adresshandels und der Adressverifizierung um die Übermittlung personenbezogener Daten gemäß § 11 Abs. 4 RBStV im Rahmen der dort in Satz 5 genannten Beschränkungen ersuchen. § 7 Abs. 2 Nr. 1 gilt entsprechend.

(3) § 14 Abs. 10 RBStV ist zu beachten.

§ 9 Technisch-organisatorischer Datenschutz

Es ist sicherzustellen, dass bei der in § 2 genannten gemeinsamen Stelle ein wirksames und übergreifendes Informationssicherheits-Managementsystem installiert und die Löschung der Daten von Rundfunkteilnehmern und Beitragsschuldnern nach einem einheitlichen Konzept geregelt wird.

12.6 Liste der Datenschutzbeauftragten (AK DSB)

Rundfunkanstalt	Datenschutzbeauftragte/r
ARTE Deutschland TV GmbH	Christoph Weber
Bayerischer Rundfunk	Axel Schneider Monika Moser
Deutsche Welle	Thomas Gardemann
Deutschlandradio	Ulla Pageler
Hessischer Rundfunk	Ulrich Göhler Simone Schlee
Kinderkanal ARD/ZDF	Jörn Voss
Mitteldeutscher Rundfunk	Stephan Schwarze Matthias Meincke
Norddeutscher Rundfunk	Dr. Heiko Neuhoff
Österreichischer Rundfunk	Rainer Rauch
Radio Bremen	Anna-Katharina Puschmann
Rundfunk Berlin Brandenburg	Anke Naujock-Simon
Saarländischer Rundfunk	Marion Klein
Südwestrundfunk	Prof. Dr. Armin Herb Referat: Florian Schad
Westdeutscher Rundfunk	Karin Wagner Referat: Günter Grießbach
Zweites Deutsche Fernsehen	Gerold Plachky
Zentraler Beitragsservice	Katharina Aye Christian Kruse

12.7 Liste der Mitglieder der Rundfunkdatenschutzkonferenz (RDSK)

Rundfunkanstalt	Rundfunddatenschutzbeauftragte/r
Bayerischer Rundfunk, Deutschlandradio, Saarländischer Rundfunk, Zweites Deutsches Fernsehen, Westdeutscher Rundfunk	Dr. Reinhart Binder
Deutsche Welle	Thomas Gardemann
Hessischer Rundfunk	Ulrich Göhler Simone Schlee
Mitteldeutscher Rundfunk	Stephan Schwarze
Norddeutscher Rundfunk	Dr. Heiko Neuhoff
Radio Bremen	Anna-Katharina Puschmann
Rundfunk Berlin Brandenburg	Anke Naujock-Simon
Südwestrundfunk	Prof. Dr. Armin Herb

12.8 Positionspapiere der Rundfunkdatenschutzkonferenz

RDSK
RUNDFUNKDATENSCHUTZKONFERENZ

Diskussionspapier der Konferenz der Datenschutzaufsichtsbehörden der Rundfunkanstalten (RDSK) zum SAP-Gesamtprojekt

---

Das ARD Strukturprojekt „SAP Prozessharmonisierung“ weist mit einer Unterteilung in 30 Teilprojekte und einer Vielzahl beteiligter Personen der Rundfunkanstalten eine hohe Komplexität auf. Ziel des Projektes ist die Vereinheitlichung von Abläufen mit den am Projekt teilnehmenden Häusern. Die IT-gestützten betriebswirtschaftlichen Geschäftsprozesse, insbesondere zu Finanzen, Controlling, Personalwesen, Einkauf/Vertragswesen, Honorare sowie Rechte und Lizenzen sollen über einen Zeitraum von 10 Jahren angeglichen werden.

Das folgende Diskussionspapier der Rundfunkdatenschutzkonferenz (RDSK) beschäftigt sich mit den Anforderungen, insbesondere der EU Datenschutz-Grundverordnung (DSGVO) zum Schutz personenbezogener Daten. Diese sind von allen am Gesamtprojekt beteiligten **Rundfunkanstalten** einzuhalten, weil sie jeweils **für die Verarbeitung verantwortlich** sind (Art. 24 DSGVO). Zudem sind klare Strukturen und Rollen (auch im Hinblick auf die Aufgaben der Projektleitung) bei der Umsetzung der datenschutzrechtlichen Vorgaben notwendig. Die jeweils für den Datenschutz zuständigen Stellen der einzelnen Rundfunkanstalten sind frühzeitig einzubeziehen.

1. Vertragliche Erfordernisse
   - Bei Shared Services sind im Rahmen einer **Joint Controller Vereinbarung** gemäß Artikel 26 DSGVO Verantwortlichkeiten festzulegen, z.B. Ansprechpartner für Betroffenenrechte (z.B. Auskunftsrecht) oder Regelungen zu den Meldepflichten bei Datenschutzpannen
     - Regelungen für die eingeschränkte Verarbeitung von Daten (gesperrte Daten), damit diese Daten nur von einem eingeschränkten Personenkreis verarbeitet werden dürfen

- Regelungen zum Verbot der Profilbildung und damit auch das Gebot Auswertungen nur statistisch/anonym durchzuführen
- Die Datenverarbeitung sollte möglichst nur innerhalb der EU stattfinden und die Art. 44 ff. DSGVO berücksichtigen (und Bewegungsdaten, welche die EU verlassen, sollten verschlüsselt transportiert werden); sofern allerdings sensible Daten (z.B. Personaldaten) betroffen sind, hat die Verarbeitung im Geltungsbereich der DSGVO zu erfolgen
- Die technischen und organisatorischen Maßnahmen (TOMs) der beteiligten Rundfunkanstalten zur Sicherheit der Daten (Artikel 32 DSGVO) müssen festgelegt werden

- Der oder die **Auftragsdatenverarbeitungsverträge** haben den Anforderungen nach Artikel 28 DSGVO zu genügen und es soll das AV-Vertragsmuster der öffentlich-rechtlichen Rundfunkanstalten verwendet werden.

  Es müssen insbesondere Regelungen enthalten sein, welche die folgenden Sachverhalte betreffen:

  - Gewährleistung der Betroffenenrechte
  - Subunternehmer (Unterauftragsverarbeiter) sind zu benennen und diesen sind die Regelungen des AV-Vertrages ebenfalls aufzuerlegen
  - Die Verarbeitung sensibler Daten darf nur in der EU stattfinden; deshalb dürfen z.B. auch Personaldaten nicht in eine US-Cloud gespeichert werden, zumal zu erwarten ist, dass das so genannte Privacy Shield vom Europäischen Gerichtshof aufgehoben wird.
  - Die Kontrollrechte der Rundfunkbeauftragten für den Datenschutz müssen gewahrt werden
  - Der Ausschluss eines Zurückbehaltungsrechts an Daten ist zu vereinbaren
  - Es sind Vertraulichkeitsklauseln aufzunehmen
  - Es muss gewährleistet sein, dass die Daten aus der Cloud wieder auf Rechner in den Rundfunkanstalten rückholbar sind

2. Weitere generelle Anforderungen an alle Module im SAP-Paket sind:
   - Es hat eine Klassifizierung der Daten zu erfolgen, da davon die Anforderungen an die konkrete Verarbeitung abhängen, insbesondere der Schutzbedarf und die daraus resultierenden technischen und organisatorischen Maßnahmen
   - Es sind Möglichkeiten zur Löschung von Daten vorzusehen
     - Je nach Modul sind Fristen für die Löschung einzubauen
     - Regelungen für die Behandlung der Logdaten der Mitarbeiter sind erforderlich

- Berechtigungskonzepte (auch im Hinblick auf eine eingeschränkte Verarbeitung) müssen implementiert werden
- Auswertungen haben grundsätzlich ohne Personenbezug zu erfolgen
- Das Recht auf Datenübertragbarkeit (Datenportabilität) muss gewährleistet sein (z.B. bei Mitarbeiterwechsel innerhalb der ARD)
- Es ist ein Prozess einzurichten, der die Datensicherheit stets auf dem aktuellen Stand der Technik sicherstellt
- Sofern vorhanden sind zertifizierte Produkte einzusetzen

3. Die Einhaltung der Vorgaben ist entsprechend Art. 5 Abs. 2 DSGVO zu dokumentieren und nachzuweisen.

13. Dezember 2019, Version 3.1

RDSK
RUNDFUNKDATENSCHUTZKONFERENZ

Empfehlung der RDSK zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten

---

Das Urteil des EuGH vom 1. Oktober 2019 – C 673/17 – in der Sache „Planet 49“ konkretisiert die Anforderungen an eine wirksame Einwilligung zur Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind. Es hat vermehrt zu Fragen zur Zulässigkeit des Einsatzes von Cookies in den Online-Angeboten der Rundfunkanstalten geführt. Die wichtigsten Grundsätze dazu sind hier unter I., einige Handlungsempfehlungen für die Rundfunkanstalten unter II. zusammengefasst.

I. ZULÄSSIGKEIT VON COOKIES

Nach Art. 6 der EU-Datenschutz-Grundverordnung kann der Einsatz von Cookies über eine Einwilligung oder über andere Erlaubnistatbestände gerechtfertigt sein:

1. Allgemeiner Erlaubnistatbestand: Einwilligung der betroffenen Person

Ist keine gesetzliche Ermächtigung einschlägig (siehe Ziff. 2) darf der Verantwortliche ein Cookie nur mit der ausdrücklichen Einwilligung der betroffenen Person einsetzen (Opt-In).

Auf eine solche Einwilligung kann sich der Verantwortliche berufen, wenn die betroffene Person die entsprechende Erklärung a) zweifelsfrei aktiv, b) freiwillig und c) in Kenntnis aller für die Datenverarbeitung relevanten Umstände abgegeben hat.

Diese Voraussetzungen sind im allgemeinen nur dann erfüllt, wenn der Verantwortliche die Person über die mit dem Cookie verbundene Datenverarbeitung umfassend informiert hat und ihr die Möglichkeit gibt, das Einverständnis durch eigenes Handeln bzw. eine eigene Willenserklärung, etwa durch Ankreuzen eines entsprechenden Kästchens, zu erteilen, ohne dass sie im Falle der Ablehnung mit Nachteilen rechnen muss.

Die Person muss die Einwilligungserklärung leicht als solche erkennen können. Das schließt zwar nicht aus, dass der Verantwortliche sie mit weiteren Willensbekundungen verbindet. Dann muss die Einwilligungserklärung aber von den anderen Sachverhalten klar unterscheidbar sein.

Eine Einwilligung kann sich auch auf mehrere Cookies beziehen, wenn diese jeweils denselben Zweck verfolgen.

1. Besondere Erlaubnistatbestände

a) Unbedingt erforderliche Cookies

Eine Einwilligung ist nicht nötig, wenn die mit dem Einsatz des Cookies verbundene Speicherung oder der Zugang zu den entsprechenden Daten unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Danach bedürfen jedenfalls sogenannte ‚funktionale Cookies' keiner Einwilligung,

die etwa

- dem Verantwortlichen eine (technische) Fehleranalyse ermöglichen,
- der Sicherheit seines Angebots dienen,
- die Login-Daten seiner Nutzer speichern,
- für Transaktionen (Warenkorbfunktion) oder
- zur Individualisierung von Webseiteninhalten erforderlich sind.

b) Sonstige Cookies

Bisher erlaubt § 15 Abs. 3 TMG dem Verantwortlichen die Auswertung pseudonymisierte Nutzungsdaten der betroffenen Person für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung seines Online-Angebots auch ohne Einwilligung der betroffenen Person (Opt-Out). Allerdings dürfte diese Vorschrift mit dem europäischen Recht nicht mehr vereinbar sein.

Die Verarbeitung personenbezogener Daten kann jedoch auch durch einen der Erlaubnistatbestände gerechtfertigt sein, die Art. 6 Abs. 1 S. 1 lit. b) bis f) DSGVO nennt. Diese betreffen jeweils sehr spezifische Konstellationen und kommen deshalb für den Einsatz von Cookies nur in besonders gelagerten Fällen in Betracht. Nach dem Urteil des EuGH vom 1.10.2019 kann das allgemeine Interesse des Verantwortlichen an einer Er-

fassung und Auswertung des Nutzungsverhaltens (insbesondere in den in § 15 Abs. 3 TMG genannten Fallgruppen) nicht per se als „berechtigtes Interesse“ im Sinne von Art. 6 Abs. 1 S. 1 lit. f) DSGVO qualifiziert werden. Hier bedarf es einer sorgfältigen Abwägung mit den Interessen und Grundrechten der betroffenen Personen.

c) Insbesondere: Nutzungsmessung des öffentlich-rechtlichen Rundfunks

Der öffentlich-rechtliche Rundfunk verbreitet Telemedien, um seinen verfassungs- rechtlichen Funktionsauftrag zu erfüllen. Nach der Rechtsprechung des Bundesverfassungsgerichts darf (und muss) er sein von den Beitragszahlern finanziertes An- gebot im gesellschaftlichen Interesse auf allen publizistisch relevanten Plattformen zugänglich machen. Ob, wo und wie er damit seinen publizistischen Auftrag erfüllt, hängt von der Konfiguration dieses Angebots ab. Die Rundfunkanstalten sind dazu auf Erkenntnisse zur Akzeptanz und Nutzung ihres Angebots angewiesen. Dies gilt allerdings ausschließlich für anonymisierte Auswertungen, wie sie auch im linearen Rundfunk üblich sind. Vergleichbar statistisch belastbare Methoden wie etwa die Messung der Zuschauerquoten (Fernsehen) oder die Media-Analyse (Hörfunk) stehen dafür im Online-Bereich jedoch bislang nicht zur Verfügung. Die Rundfunkanstalten haben daher im Rahmen ihres verfassungsrechtlichen Funktionsauftrags ein berechtigtes Interesse am Einsatz von Cookies, die diese Aufgabe für ihr Onlineangebot übernehmen. Sie verfolgen damit also kein (markt-)wirtschaftliches, sondern ein ausschließlich publizistisches Ziel, und die anonymisierte Nutzungsmessung ist zudem erforderlich, damit sie die ihnen durch Art. 5 Abs. 1 S. 2 GG übertragene Aufgabe optimal wahrnehmen können, Art. 6 Abs. 1 S. 1 lit. e) bzw. f) DSGVO.

II. EMPFEHLUNGEN FÜR DIE RUNDFUNKANSTALTEN

Rechtsgrundlage prüfen

Die Rundfunkanstalten sollten jedes von ihnen eingesetzte Cookie darauf überprüfen, ob sie es auf einen Erlaubnistatbestand stützen können. Dies kann einer der in Art. 6 Abs. 1 S. 1 lit. b) – f) DSGVO genannten Tatbestände und muss ansonsten stets eine Einwilligung der betroffenen Person sein.

Die RDSK empfiehlt den Rundfunkanstalten, den Einsatz von Cookies nicht (mehr) auf § 15 Abs. 3 TMG zu stützen.

Wirksamkeit der Einwilligungserklärung sichern

Die Rundfunkanstalten sollten die von ihnen eingesetzten Tools, mithilfe derer sie die im Regelfall erforderliche Einwilligung der betroffenen Person einholen, darauf- hin überprüfen, ob sie die Anforderungen erfüllen, die sich aus Art. 4 Nr. 11, Art. 7 und ggf. Art. 8 DSGVO und der Rechtsprechung des EuGH ergeben.

Datenschutzerklärung/Cookie-Hinweis anpassen

Die Datenschutzerklärung muss Hinweise zur Funktion des jeweiligen Cookies mit mindestens allen Angaben enthalten, die Art. 13 DSGVO fordert.

Spezifische Aufgabe des öffentlich-rechtlichen Rundfunks erklären

Zu Recht erwarten die Nutzer vom öffentlich-rechtlichen Rundfunk einen besonders hohen Datenschutzstandard. Da im Allgemeinen gerade Cookies, die das Nutzungs- verhalten erfassen und auswerten, nur mit ausdrücklicher Einwilligung der betroffenen Person eingesetzt werden dürfen, entsteht erhöhter Aufklärungs- und Beratungsbedarf, wenn die Rundfunkanstalten weiterhin für einzelne Cookies keine Einwilligung einholen. Sie sollten daher ihre Datenschutzerklärungen bzw. Cookie-Hinweise besonders sorgfältig und verständlich formulieren. Allgemeinplätze wie etwa das Bestreben, mithilfe eines Cookies „den Nutzern ein bestmögliches Angebot zur Verfügung zu stellen“, werden dem nicht gerecht. Insbesondere sollten die Rundfunkanstalten daher die spezifische Aufgabe und Funktion des öffentlich-rechtlichen Rundfunks erläutern und die sich daraus ergebende Rechtsgrundlage für den Einsatz des betreffenden Cookies nennen.

Februar 2020

RDSK
RUNDFUNKDATENSCHUTZKONFERENZ

Positionspapier der Rundfunkdatenschutzkonferenz (RDSK) zum IP-Autostart bei der Nutzung von HbbTV

Bei HbbTV (Hybrid Broadcast Broadband TV) kann sowohl das Rundfunksignal (Broadcasting) als auch das Breitbandinternet (Broadband) genutzt werden, um den Fernsehzuschauerinnen und -zuschauern neben der Rundfunksendung weitere Zusatzinformationen anzubieten. Bei Nutzung des Breitbandinternets wird bereits bei Aufruf eines Senders mittels einer über das Rundfunksignal versandten URL automatisch eine Internet-Verbindung zum Server des HbbTV-Anbieters hergestellt. Dadurch werden die Zusatzinformationen schon vor dem Drücken des Red-Buttons auf der Fernbedienung im Hintergrund geladen. Dies ist bei Nutzung der Online-Verbindung vom HbbTV-Standard so zwingend vorgegeben und hat u.a. zur Folge, dass die Zusatzangebote den Zuschauerinnen und Zuschauern unmittelbar nach dem Drücken des Red-Button ohne zeitliche Verzögerung zur Verfügung stehen.

Die Rundfunkdatenschutzkonferenz (RDSK) vertritt dazu folgende Rechtspositionen:

Die Datenverarbeitung im Zusammenhang mit der Verbreitung von Rundfunkangeboten im HbbTV–Standard ist von der Öffnungsklausel in Art. 85 Abs.

1. EU-Datenschutzgrundverordnung (DSGVO) erfasst. Sie unterliegt daher der Kontrolle der rundfunkspezifischen Datenschutzaufsicht. Auch bei den Rundfunkanstalten mit einer gespaltenen Kontrollzuständigkeit (Radio Bremen, Hessischer Rundfunk, Rundfunk Berlin-Brandenburg und Deutsche Welle) sind die Angebote von einer staatlichen Aufsicht ausgenommen und unterliegen ausschließlich der Kontrolle der Datenschutzbeauftragten der Rundfunkanstalten.
2. HbbTV gehört zum gesetzlichen Auftrag der öffentlich-rechtlichen Rundfunkanstalten. Das folgt aus der verfassungsrechtlich verbrieften Bestands- und Entwicklungsgarantie des öffentlich-rechtlichen Rundfunks.
3. Der IP-Autostart ist auch nach Wirksamwerden der DSGVO rechtlich zulässig. Rechtsgrundlage für den IP-Autostart ist Art. 6 Abs. 1 lit. e) DSGVO in Verbindung mit den gesetzlichen bzw. staatsvertraglichen Aufgabenzuweisungen an die Rundfunkanstalten. Außerdem können sich die Rundfunkanstalten auch auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO („berechtigtes Interesse“) stützen.

4. Für die effiziente Nutzung der hybriden Zusatzangebote ist der IP-Autostart erforderlich. Nur auf diese Weise ist gewährleistet, dass die Nutzung der Zusatzangebote unmittelbar nach dem Drücken des Red-Button beginnen kann.

Würde die IP-Verbindung erst nach dem Drücken des Red-Button aufgebaut, käme es zu einer unzumutbaren Verzögerung bei der Nutzung der Zusatzangebote. Zudem ist bei der DSMCC-Option die Speicherung einer Zustimmung der Nutzerin / des Nutzers nur bei einem kleinen Prozentsatz der Geräte möglich. Auch wäre eine Reihe von HbbTV-Zusatzangeboten (z.B. Internet Link Services bei DVB T2, Hinweisdienste etc.) nur noch mit signifikanten Umwegen für die Zuschauer zu realisieren. Außerdem käme es aufgrund der begrenzten Bandbreite zu nicht hinnehmbaren inhaltlichen Einschränkungen in der Darstellung und im Umfang des Angebots.

5. Ausweislich des „Digitalisierungsberichts 2019 Video“ verfügt inzwischen die Mehrheit der TV-Haushalte über ein internetfähiges TV. Das Angebot von hybriden Zusatzdiensten ist mittlerweile Standard. Der Anteil der on-demand genutzten TV- Inhalte (Mediatheken) steigt stetig. Mit diesen Entwicklungen hat sich auch das Bewusstsein der Zuschauerinnen und Zuschauer verändert. Ihnen ist bewusst, dass bereits mit der bei Installation ihres Gerätes hergestellten Verbindung zum Internet die Möglichkeit der Übertragung der IP-Adresse eröffnet ist. Wer sein Fernsehgerät mit dem Internet verbindet, der weiß, dass eine Kommunikation nur über eine IP- Adresse möglich ist. HbbTV ist heute der mit Abstand wichtigste und am meisten genutzte Weg zur Darstellung der öffentlich-rechtlichen Mediatheken auf TV-Geräten.

6. Die RDSK weist darauf hin, dass die IP-Adresse vor dem Drücken des Red-Button ausschließlich zur Übertragung von Zusatzangeboten und nicht zur Bildung von Nutzerprofilen genutzt werden darf.

Stand: Dezember 2019

12.9 Jahresbericht 2019 des bDSB für den Kinderkanal von ARD/ZDF

1. bDSB – Weiterbildungen, Tagungen und Veranstaltungen	
19.02	GDD, Planung und Umsetzung der Überwachungsaufgabe des DSB
19.10	Zertifizierung zum bDSB GDDcert. EU

2. Audits im KiKA	
19.11	Jährliches Datenschutzgespräch im KiKA

3. Arbeitskreise und -gemeinschaften	
19.02	AK DSB, DW Bonn (Sondersitzung)
19.04	AK DSB, RB Bremen #1/2
19.11	AK DSB, BR München #2/2
19.03	MDR Datenschutzkoordinatoren #1/3
19.07	MDR Datenschutzkoordinatoren #2/3
19.12	MDR Datenschutzkoordinatoren #3/3

4. Organisatorische Maßnahmen	
19.01	Handlungsanweisung FA. Peakperformance zum Thema „Löschprotokoll-Adventsshow“
19.03	Aktualisierung Einverständniserklärungen Besuchertag
19.04	Handlungsanweisung FA. Peakperformance zum Thema „Löschprotokoll-Dein Song 2019“
19.09	Handlungsanweisung FA. Peakperformance zum Thema „Löschprotokoll-Dreamteam 2019“
19.09	Privacy by Design – kika.de „Datenschutz-Icons“
19.10	Handlungsanweisung FA. Peakperformance zum Thema „Löschprotokoll-Pausengames“
19.10	EU-Cookieentscheidung – Umgang im Sender

5. Abgeschlossene red.spezifische Aufgaben und Problemstellungen		Redaktion
19.01	DbKD Mitmachaktion	200
19.01	Spam-Werbung RoberBoschStiftung-Datenschutz	200.600
19.01	AVV - FA. Exozet	200.700
19.01	Div. Aktualisierungen Datenschutzerklärung auf kika.de	200.700
19.01	Applestore – Klärung Nutzung der KiKA-Produkte im Koreanischen-Appstore	110
19.02	AVV - FA. Peakperformance	200
19.02	eSponse - Datenmissbrauchsmeldung	200.600
19.02	KiKA Live – Aktion „Dreamteam“	210
19.02	Kummerkasten – Aktion „Liebesbotschaften“	210

19.02	Div. Aktualisierungen Datenschutzerklärung auf kika.de	200.700
19.03	Aktion – „KiKA kommt zu Dir“	210
19.03	Anpassung – Kontaktformular Elternseiten	200.600
Abgeschlossene red.spezifische Aufgaben und Problemstellungen		Redaktion
19.03	KiKA live – Aktion „Pausengames“	210
19.03	Div. Aktualisierungen Datenschutzerklärung auf kika.de	200.700
19.03	AVV - EBU	110
19.03	B2B-Fragebogen KiKA Unternehmenskommunikation	100
19.04	Datenschutzkonzept „Instagram“	200.600
19.04	Überarbeitung Webtalk	200
19.04	B2B – Umfrage über Presselounge	100
19.04	KiKA Dein Song 2019 - Löschung der Daten Online Voting	210
19.05	Nutzung der Suchmaschine „Ecosia“	100
19.05	Antwortverhalten Google PlayStore	110
19.05	AVV – FA. MitX-perts – hbbTV Hosting	200
19.06	Mitmachaktion „Schloss Einstein“	200
19.06	eSponse - Löschungssystematik	200.600
19.07	Div. Aktualisierungen Datenschutzerklärung auf kika.de	200.700
19.07	Einverständniserklärung „Planpunkt“	110
19.08	Kikaninchen-App Auswertung techn. Parameter	240
19.08	Div. Aktualisierungen Datenschutzerklärung auf kika.de	200.700
19.08	Aktion - Audiomitschnitt eines Chors und dessen Upload	210
19.08	Kummerkasten – Aktion „Coaching Aufruf“	210
19.08	Timster – Aktion „Digitales Klassenzimmer“	210
19.08	Kikaninchen – Aktion „ Geburtstagslied KiKaninchen“	240
19.08	KiKA Tanzalarm Club - Kommentarvorhaben	210
19.08	Timster - Datenabfrage	210
19.10	Timster - Weitergabe O-Töne	210

6. Externe Unterstützungsanfragen		
19.01	AVV in Auftragsproduktionsverträgen	MDR
19.04	MDR Jump Osterfeuervoting - Löschung der Daten & Anfertigung Löschprotokoll	MDR
19.06	AVV InfOnline	HR
19.09	HbbTV-VTX-Mandant Datenschutzerklärung	KiKA/POC
19.11	Datenschutzerklärung „Sandmann-Voting“	rbb

6. Laufende senderspezifische Problemstellungen		Redaktion
	Keine	

7. Auskunftsersuche	
19.01	Auskunftsersuchen Einverständniserklärung bei Besuchen
19.01	Geofencing des KiKA-Player
19.03	Auskunft zu TikTok – Nachrichtensendung logo vom 04.03.19
19.06	Ene Mene Bu - Bildergalerie
19.09	Allgem. Auskunftsersuchen

8. Strafverfolgungen	
19.02	Droh-Email
19.04	Suizidandrohung in Chat
19.11	Droh-Email

9. spezielle Mitarbeitersensibilisierung		Redaktion
19.03	eSponse – Datenschutzgespräch mit FA. Dialsystems und Redaktion	200.600

10. Diskutierte Hauptthemen im AK DSB (nach Sendern geordnet)		Sender
19.01	Facebook-Termin: Präsentation und Organisatorisches	BR
19.01	EuGH-Urteil und Vereinbarung im Sinne von Art. 26 DS-GVO	BR
19.08	Facebook Lead Ads	HR
19.03	Entwurf eines novellierten Rundfunkbeitragsstaatsvertrages - Mündliche Anhörung am 29. April 2019 in Berlin	NDR
19.06	Rechtsauffassung der DSK zur Anwendbarkeit der Orientierungshilfe des DÜS Kreises für Smart-TV Dienste	RB
19.06	Chartbeat	RB
19.01	Beschäftigtendatenschutz	rbb
19.02	Online-Nutzungsmessung und Firefox	rbb
19.04	Auftragsverarbeitung - DS 7.7.2	rbb
19.07	Joint Controller-Vereinbarung ZBS	rbb
19.07	Betriebliche oder Behördliche Datenschutzbeauftragte?	rbb
19.07	Scribble Live	rbb
19.08	Orientierungshilfe des Düsseldorfer Kreises für Anbieter von Telemedien zum Thema Smart-TV-Dienste	rbb
19.09	Dienstleistungs- und Maklervertrag für betrieblich gestützte Versorgungssysteme BVUK	rbb
19.02	Rahmenvereinbarung Office 365	SWR
19.06	Medienprivileg und Bildnisschutz	SWR
19.07	A-1 Bescheinigung bei Entsendung von Mitarbeitern ins Ausland - DS 19.38	SWR
19.10	Power eCard	WDR
Diskutierte Hauptthemen im AK DSB (nach Sendern geordnet)		Sender
19.10	UCL MD4 Police screening Signage	WDR
19.05	Nielsen AVV	ZDF
19.03	Entwurf Vereinbarung zur gemeinsamen Verantwortlichkeit	Zentraler Beitragsservice