

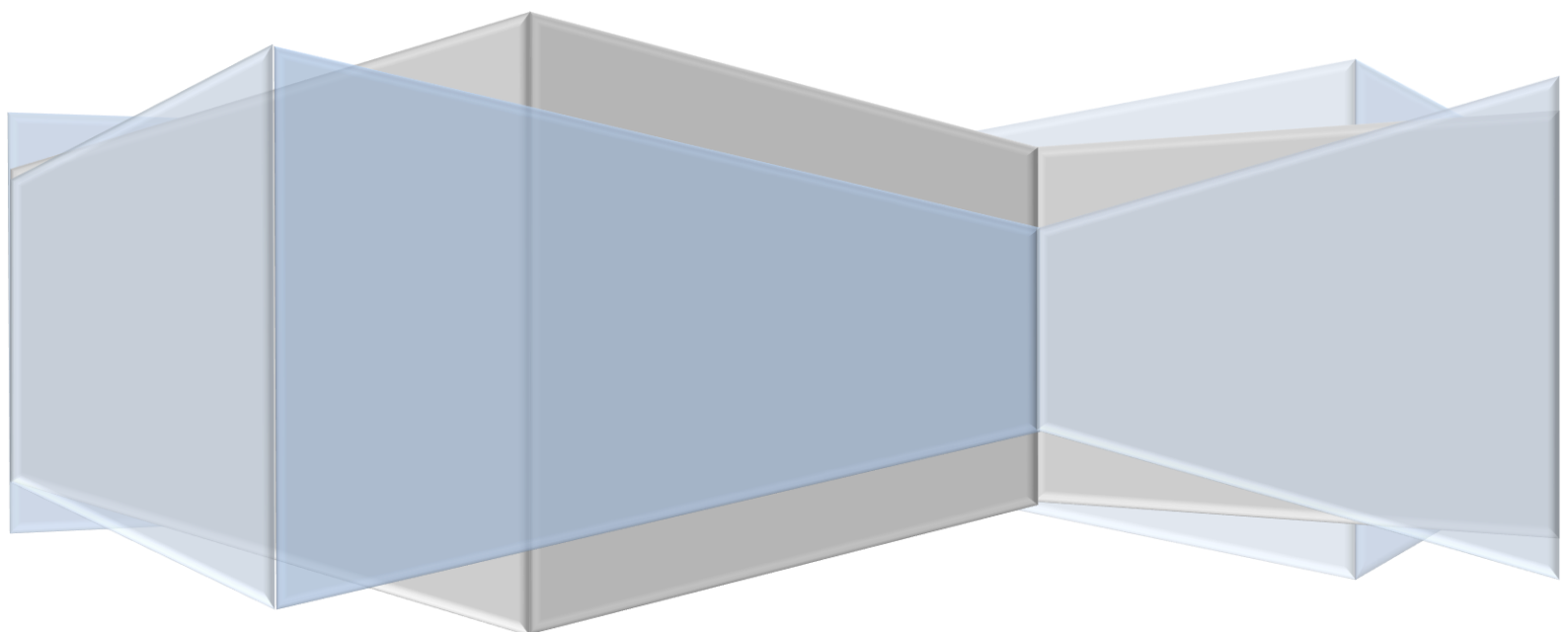


MITTELDEUTSCHER RUNDFUNK
Anstalt des öffentlichen Rechts

Tätigkeitsbericht des Rundfunkdatenschutz- beauftragten des MDR

Zeitraum 01.01.2021 bis 31.12.2021

Stephan Schwarze



Inhaltsverzeichnis

1. Einleitung.....	4
2. Aufgaben des Rundfunkdatenschutzbeauftragten.....	6
2.1. Aufgaben und Befugnisse	6
2.2. Eingaben beim Rundfunkdatenschutzbeauftragten	8
2.3. Klage gegen einen Bescheid des Rundfunkdatenschutzbeauftragten.....	9
3. Entwicklung des Datenschutzrechts im Jahre 2021	10
3.1. Europäische Datenschutzgrundverordnung	10
3.2. E-Privacy-Verordnung	10
3.3. EU-Standardvertragsklauseln	11
3.4. Brexit	11
3.5. IT-Sicherheitsgesetz 2.0.....	12
3.6. Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDGS)	12
3.7. Urteil des OVG Schleswig-Holstein vom 25.11.2021 zur Untersagung des Betriebs einer Facebook-Fanpage	14
4. Datenschutz beim MDR	15
4.1. Neue Standardvertragsklauseln	15
4.2. Kontrolle des Arbeitgebers des 3G-Status	16
4.3. Interaktives Hörspiel	16
4.4. Einsatz von MS Teams.....	17
4.5. Auslagerung und Beratung zur Pensionskasse	18
4.6. Mal wieder: Cookies	19
5. Datenschutz beim KiKA	21
5.1. Zusammenarbeit mit dem KiKA	21
5.2. KiKA Quiz-APP	21
5.3. Datenschutzvorfall Presselounge	22
6. Datenschutz beim Zentralen Beitragsservice	24
6.1. Datenschutz im Zusammenhang mit dem Rundfunkbeitrag	24
6.2. Umsetzung des Löschkonzeptes.....	25
7. Datenschutz im IVZ	25
7.1. Datenschutz im Informationsverarbeitungszentrum (IVZ).....	25
8. Datenschutz bei Tochterfirmen des MDR	26
8.1. Datenschutzvorfall bei der AVI.DAT Software und Technologie GmbH	26

9.	Rundfunkdatenschutzkonferenz (RDSK).....	28
9.1.	Grundsätzliches.....	28
9.2.	Funktion der RDSK.....	28
10.	Zusammenarbeit im Arbeitskreis der Datenschutzbeauftrag- ten von ARD, ZDF und Deutschlandradio (AK DSB)	30
10.1.	Zusammenarbeit im AK DSB.....	30
10.2.	Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten der Rundfunkanstalten	31
11.	Schlussbemerkungen.....	33
12.	Anhang	34
12.1.	MDR-Staatsvertrag (§§ 36 bis 40)	34
12.2.	MDR-Datenschutzsatzung	40
12.3.	Artikel 85 EU-Datenschutz-Grundverordnung (DSGVO)	44
12.4.	Rundfunkbeitragsstaatsvertrag (§§ 11 und 14)	45
12.5.	MDR-Rundfunkbeitragsatzung (§§ 7 bis 9)	48
12.6.	Liste der Datenschutzbeauftragten (AK DSB).....	50
12.7.	Liste der Mitglieder der Rundfunkdatenschutzkonferenz (RDSK).....	51
12.8.	Positionspapiere der Rundfunkdatenschutzkonferenz	52
12.9.	Verwaltungsvereinbarungen zur Wahrung der Datenschutzaufsicht über Gemeinschaftsunternehmen und –einrichtungen der Rundfunkanstalten	59
12.10.	Jahresbericht 2021 des bDSB für den Kinderkanal von ARD/ZDF	71

1. Einleitung

Der Rundfunkdatenschutzbeauftragte hat den Organen des MDR jährlich einen schriftlichen Bericht gemäß Artikel 59 der DSGVO über seine Tätigkeit zu erstatten. Mit dem vorliegenden Bericht komme ich meiner Pflicht aus § 40 Abs. 4 MDR-Staatsvertrag nach. Mit diesem Bericht soll ein Überblick gegeben werden über die Tätigkeit des Rundfunkdatenschutzbeauftragten im Jahr 2021.

Das Thema Pandemie hat uns auch im Jahr 2021 begleitet. Die Frage, wie datenschutzrechtlich auf die Anforderungen des Infektionsschutzgesetzes reagiert werden muss und wie möglichst sorgsam mit Gesundheitsdaten umgegangen werden kann, war ein wichtiges Thema. Die Zusammenarbeit mit dem betrieblichen Datenschutzbeauftragten sowie den Verantwortlichen des MDR musste teilweise schnell organisiert werden und hat gut funktioniert.

In diesem Jahr mussten keine Beanstandungen in förmlicher Hinsicht ausgesprochen werden. Neue Themen kommen hinzu und nicht immer läuft alles reibungslos. Aufsichtsrechtliche Maßnahmen waren aber nicht vonnöten. Die Einbeziehung des Verwaltungsrates konnte damit unterbleiben und eine Unterrichtung der Gremien wird durch diesen Tätigkeitsbericht umgesetzt.

Der operative Datenschutz obliegt dem betrieblichen Datenschutzbeauftragten des MDR, Herrn Matthias Meincke, dem ich aufgrund der nun schon einige Jahre währenden vertrauensvollen Zusammenarbeit zu Dank verpflichtet bin. Gleiches gilt für Herrn Dr. Bernd Appel als Abwesenheitsvertreter des betrieblichen Datenschutzbeauftragten sowie für meine Assistentin Frau Kirsten Schmidt, die zuverlässig und kreativ und in kompetenter Weise die allfälligen Arbeiten im Büro erledigt hat. Allen Genannten möchte ich meinen herzlichen Dank aussprechen.

Die Datenverarbeitungen der Beteiligungsunternehmen des MDR sowie des Kinderkanals von ARD und ZDF unterstehen ebenfalls meiner Aufsicht. Bei einem Tochterunternehmen war ein geringfügiger Datenschutzvorfall zu verzeichnen, über den ich berichten werde. Die Innovation-Digital-Agentur GmbH (ida) wird im Jahr 2022 ihre Dienstleitung für den MDR in vollständiger Weise übernehmen. Damit

auch in datenschutzrechtlicher Hinsicht alles reibungslos verläuft, begleiten Herr Meincke und ich diesen Prozess.

Herr Jörn Voss ist nach wie vor betrieblicher Datenschutzbeauftragter des Kinderkanals. Für die Zusammenarbeit, die auch in diesem Jahr problemlos und vertrauensvoll war, darf ich mich an dieser Stelle herzlich bedanken.

Die Rundfunkdatenschutzbeauftragten sowie die betrieblichen Datenschutzbeauftragten im öffentlich-rechtlichen Rundfunk arbeiten in der Rundfunkdatenschutzkonferenz sowie im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio zusammen. Im Berichtsjahr fanden wiederum keine Präsenzsitzungen statt, sondern Videokonferenzen. Dies hat sich mittlerweile gut eingespielt und konnte sogar noch ausgeweitet werden. Es hat sich gezeigt, dass die Themen so vielfältig und teilweise eilbedürftig sind, dass ein regelmäßiger Jour fixe neben den umfangreichen Sitzungen Sinn ergibt.

Im Jahr 2022 wird der Vorsitz des AK DSB auf den Bayerischen Rundfunk und das ZDF wechseln, so dass nicht mehr Herr Dr. Heiko Neuhoff vom NDR, sondern Herr Axel Schneider vom Bayerischen Rundfunk und Herr Gerold Plachky vom ZDF die Leitung des Gremiums übernehmen werden.

Datenschutz bleibt ein wichtiges Thema und die Fragen sind immer wieder neu und spannend. Gerade aktuelle Urteile eröffnen neue Perspektiven auf die rechtliche Beurteilung verschiedener Konstellationen. Für den öffentlich-rechtlichen Rundfunk ist immer interessant, inwieweit man das Spannungsfeld zwischen Rundfunkfreiheit und Datenschutz auflöst und die Grenzen in der angemessenen Weise zieht. Die Arbeit als Rundfunkdatenschutzbeauftragter macht Freude. Daher bin ich dankbar, diese Aufgabe nach wie vor erfüllen zu können.

2. Aufgaben des Rundfunkdatenschutzbeauftragten

2.1. Aufgaben und Befugnisse

Nach § 38 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 unabhängig ausgestaltet, es unterliegt insbesondere keiner Rechts- oder Fachaufsicht. Die vom Verwaltungsrat ausgeübte Dienstaufsicht darf diese 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 für dessen Beteiligungsunternehmen. Die Aufgaben und Befugnisse ergeben sich aus § 40 MDR-Staatsvertrag und aus den Artikeln 57 und 58 DSGVO.

Jedermann hat das Recht, sich unmittelbar an den Rundfunkdatenschutzbeauftragten zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch den MDR oder seiner Beteiligungsunternehmen in seinen schutzwürdigen Belangen verletzt zu sein. Hinzu kommen die Aufgaben nach Artikel 57 DSGVO, wonach insbesondere 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 insbesondere umgesetzt durch die 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.

In Ergänzung dazu formuliert § 40 MDR-Staatsvertrag verschiedene weitere Aufgaben. So hat der Rundfunkdatenschutzbeauftragte gemäß Absatz 2 dieser Vorschrift die Pflicht, Datenschutzverstöße gegenüber der Intendantin zu beanstanden

und zu einer Stellungnahme aufzufordern. Eine gleichzeitige Unterrichtung des Verwaltungsrates ist ebenso vorgesehen. Von einer förmlichen Rüge kann allerdings abgesehen werden, wenn es sich um einen unerheblichen Mangel handelt oder wenn die unverzügliche Behebung sichergestellt ist; dies ist der Regelfall. Dass ein Datenschutzverstoß nicht abgestellt wurde, obwohl die Aufsicht darauf hingewiesen hat, ist bisher nicht vorgekommen, so dass eine förmliche Beanstandung gegenüber der Intendantin nicht erforderlich war. Ebenso im § 40 MDR-Staatsvertrag ist in Absatz 4 festgelegt, dass der Rundfunkdatenschutzbeauftragte einmal jährlich den Organen des MDR einen schriftlichen Bericht im Sinne von Artikel 59 DSGVO über seine Tätigkeit zu erstatten hat, was hiermit geschieht. Eine Veröffentlichung im Internet ist obligatorisch.

Die hoheitlichen Befugnisse einer Aufsichtsbehörde, zu der der Rundfunkdatenschutzbeauftragte zählt, sind in Artikel 58 DSGVO geregelt. Danach kann ein Verantwortlicher (der MDR oder seine Beteiligungsunternehmen) ggf. per Verwaltungsakt zu Handlungen oder Unterlassungen 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 (§ 40 Abs. 1 MDR-Staatsvertrag). Dies betrifft jedoch nicht die Beteiligungsunternehmen, denen gegenüber Bußgelder möglich sind.

Die Datenschutzgrundverordnung sieht überdies vor, dass zwischen Aufsicht und betrieblichem Datenschutz zu trennen ist. Dies bedeutet aber nicht, dass eine Zusammenarbeit nicht möglich wäre. Im Gegenteil, die DSGVO sieht hier ein enges Zusammenwirken vor, das beim MDR durch einen permanenten Austausch umgesetzt wird. Nach meinem Dafürhalten 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. Eingaben beim Rundfunkdatenschutzbeauftragten

Als Aufsichtsorgan ist der Rundfunkdatenschutzbeauftragte auch zuständig für die Bearbeitung von Beschwerden. Nach § 40 Absatz 5 MDR-Staatsvertrag hat jeder das Recht, sich unmittelbar an ihn zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch den MDR in seinen schutzwürdigen Belangen verletzt zu sein.

Im Jahr 2021 erreichten mich insgesamt lediglich zehn Beschwerden, die sich fast ausschließlich auf den Beitragseinzug und die vom Beitragsservice erteilten Auskünfte bezogen. Diesen Beschwerden konnte mit rechtlichen Ausführungen begegnet werden. Es drängt sich der Eindruck auf, dass die Petentinnen und Petenten sich eigentlich gegen den Rundfunkbeitragseinzug wenden wollen und den Datenschutz dementsprechend als Vehikel benutzen. Dessen ungeachtet muss jede Beschwerde in der gebotenen Sorgfalt beantwortet werden.

Auskünfte über die Datenverarbeitung des MDR, wie sie Artikel 12 ff. DSGVO vorsehen, erteilt der Rundfunkdatenschutzbeauftragte als Aufsicht nicht. Die hauptsächliche Last bei der Beantwortung von Auskunftersuchen trägt der Zentrale Beitragsservice in Köln. Insgesamt wurden im Berichtsjahr 6.888 Auskünfte erteilt. Davon entfielen auf den Mitteldeutschen Rundfunk 670. Im Vergleich zum Vorjahresbericht (in 2020 gab es insgesamt 33.379 Auskunftersuchen, 4.170 entfielen auf den MDR) zeigt sich, dass sich die Anzahl der Auskunftersuchen deutlich reduziert hat. 2020 hing das damalige erhöhte Aufkommen von Auskunftsbegehren noch mit einer konzertierten Aktion gegen den Beitragseinzug zusammen. Derartige Aktionen konnten nach Aussage des Zentralen Beitragsservice im Berichtsjahr nicht festgestellt werden. An dieser Stelle ist hervorzuheben, dass der Zentrale Beitragsservice in dieser Art von Massengeschäft sehr gute Arbeit leistet.

Wiederholt und bekräftigend ist festzuhalten, dass die Neigung zu datenschutzrechtlichen Beschwerden insgesamt im Sendegebiet des MDR nicht hoch ist. Aufgrund der strengen Zweckbindung der Datenverarbeitung und des funktionierenden Datenschutzmanagements sowohl beim Zentralen Beitragsservice als auch beim MDR bleibt wenig Raum für erfolgreiche Beschwerden.

2.3. Klage gegen einen Bescheid des Rundfunkdatenschutzbeauftragten

Im Berichtsjahr hat mich eine Klage beschäftigt, die auf einen Vorgang des Jahres 2019 zurückgeht. Ein Rundfunkteilnehmer hatte sich beschwert und die Auffassung vorgetragen, dass der Erlass von automatisierten betragsrechtlichen Festsetzungsbescheiden deswegen einen Verstoß gegen das Datenschutzrecht darstelle, weil gemäß Artikel 22 der DSGVO automatisierte Entscheidungsfindungen verboten seien, zumindest Festsetzungsbescheide nicht die entsprechenden Voraussetzungen für eine Ausnahme davon aufwiesen.

Nach meiner Auffassung hat der Betroffene verkannt, dass der Artikel 22 DSGVO bei gebundenen, also nicht im Ermessen stehenden Entscheidungen nicht anwendbar ist, die in diesem Fall das Rundfunkbeitragsrecht vorgibt. Die Datenverarbeitung bei einer automatisierten Entscheidung im Sinne der DSGVO muss auf Bewertung einzelner Aspekte einer Person gerichtet sein. Einfache „Wenn-Dann-Entscheidungen“, die mithilfe automatisierter Einrichtungen ergehen, sind dementsprechend keine automatisierten Einzelentscheidungen oder gar unzulässiges Profiling.

Der spätere Kläger war mit meiner Entscheidung nicht einverstanden und hat sich an das Verwaltungsgericht in Leipzig gewandt. Sein Antrag war auslegungsbedürftig und erschien mir und dem von mir beauftragten Anwalt als zu unbestimmt. Im Übrigen ist es nicht möglich, eine Bescheidung seiner Beschwerde im von ihm beantragten Sinne von der Aufsichtsbehörde zu erhalten. Mit anderen Worten, die Regelungen der DSGVO (Artikel 77 und 78) verleihen einem Kläger kein Recht auf eine bestimmte Entscheidung der Aufsichtsbehörde, in diesem Fall des Rundfunkdatenschutzbeauftragten. Das Beschwerderecht beschränkt sich bei der Bearbeitung von Beschwerden auf die ordnungsgemäße Befassung mit der Beschwerde, die Untersuchung des Beschwerdegegenstands sowie der Unterrichtung des Beschwerdeführers über das Ergebnis. Das Beschwerderecht ist also ähnlich dem Petitionsrecht ausgestaltet, was ein Recht auf den Bescheid eines bestimmten Inhalts bzw. auf eine bestimmte Entscheidung in der Sache nicht umfasst.

Sowohl im Hinblick auf die vom Kläger beantragte Entscheidung als auch hinsichtlich der vorgeblichen Rechtsverletzung des MDR bzw. des Beitragsservice bestanden bei der Klage keine Erfolgsaussichten.

Nach längerem Schriftverkehr mit dem Gericht hat der Kläger im Mai 2021 seine Klage zurückgezogen. Dies ist insgesamt eine erfreuliche Entwicklung und war so auch nicht anders zu erwarten. Dennoch hätte eine Entscheidung des Gerichts in der Sache durchaus Gewicht gehabt, wenn nämlich die materielle Frage, wie Artikel 22 DSGVO auszulegen ist und was eine auf einer automatisierten Verarbeitung beruhende Entscheidung sein kann, vom Gericht beantwortet worden wäre.

3. Entwicklung des Datenschutzrechts im Jahre 2021

3.1. Europäische Datenschutzgrundverordnung

Die DSGVO vom 25. Mai 2018 ist in allen Mitgliedstaaten der Europäischen Union gültig. Mit Entschließung vom 21.03.2021 hat das EU-Parlament im Rahmen einer Evaluation festgestellt, dass die Regelung dieser Verordnung positiv zu bewerten ist. Ein grundlegender Änderungs- oder Anpassungsbedarf wurde weder seitens des EU-Parlaments noch der EU-Kommission festgestellt; die Ausführungen des letzten Tätigkeitberichtes hierzu gelten überdies weiter fort.

3.2. E-Privacy-Verordnung

Bereits im letzten Bericht habe ich über die missliche Situation berichtet, dass es keine neuen Entwicklungen von Seiten des Gesetzgebers zur e-Privacy-Verordnung gibt. Die Rechtsunsicherheiten im Hinblick auf Nutzungsmessung und den Einsatz von Cookies bestehen damit fort. Die letzte Überarbeitung der e-Privacy-Richtlinie datiert aus dem Jahre 2009 und die Unklarheiten zu den eingesetzten Technologien im Bereich der Telemedien sind erheblich. Mein Kollege Prof. Dr. Armin Herb vom SWR hat in seinem 14. Tätigkeitsbericht klare Worte gefunden und das Ringen

um eine neue e-Privacy-Verordnung als Trauerspiel bezeichnet (Ziffer 1.2.1 des Berichtes – <https://www.swr.de/unternehmen/organisation/taetigkeitsbericht-2019-100.pdf>).

3.3. EU-Standardvertragsklauseln

Die EU-Kommission hat mit Durchführungsbeschluss (EU) 2021/914 vom 04.06.2021 neue Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer verabschiedet. Bereits im letzten Bericht hatte ich unter Ziffer 9.3 über das Urteil des EuGH vom 16.07.2020 zur Datenübermittlung ins Ausland berichtet („Schrems II“). Dieser Beschluss der Kommission ist eine Folge des Urteils des EuGH zur Ungültigkeit des Privacy Shield. Die neuen Standardvertragsklauseln beinhalten geeignete Garantien gemäß Artikel 46 Abs. 2 c) DSGVO, die dann zur Anwendung kommen können, wenn – wie derzeit – kein Angemessenheitsbeschluss der EU-Kommission in Bezug auf die Datenverarbeitung im Drittland vorliegt. Die neuen EU-Standardvertragsklauseln sind für verschiedene infrage kommende Konstellationen von Datenübermittlungen modular aufgebaut. Für die für den MDR besonders relevante Konstellation der Übermittlung vom Verantwortlichen an einen Auftragsverarbeiter decken die neuen Klauseln die vertraglichen Anforderungen aus Artikel 28 DSGVO für die Auftragsvereinbarung ab, sodass künftig im Falle einer Vereinbarung der Standardvertragsklauseln kein zusätzlicher Auftragsverarbeitungsvertrag geschlossen werden muss.

3.4. Brexit

Nach Austritt von Großbritannien zum 31.01.2020 aus der EU bestanden große datenschutzrechtliche Unsicherheiten, denn damit war die DSGVO nicht mehr anwendbar. Großbritannien wurde zu einem Drittland im datenschutzrechtlichen Sinne. Die EU-Kommission hat am 28.06.2021, nach entsprechenden Übergangsvereinbarungen, einen Angemessenheitsbeschluss gemäß Artikel 45 DSGVO erlassen, wodurch das Vereinigte Königreich als sicheres Drittland anerkannt wird. Es wurden allerdings auch Bedenken geäußert, ob der Datentransfer von Großbritannien

in andere Drittländer im Sinne der DSGVO ausreichend geregelt ist. Dessen ungeachtet können nun auf Basis des Angemessenheitsbeschlusses personenbezogener Daten von Deutschland aus ohne weitere vertragliche oder technisch-organisatorische Hemmnisse ins Vereinigte Königreich übermittelt werden.

3.5. IT-Sicherheitsgesetz 2.0

Bereits im letzten Bericht hatte ich unter Ziffer 3.4 zum Entwurf des 2. IT-Sicherheitsgesetzes berichtet. Dieses IT-Sicherheitsgesetz trat im Mai 2021 in Kraft. Zur Erhöhung der Sicherheit werden die Befugnisse des Bundesamtes für Informationssicherheit (BSI) gestärkt und Rechte und Pflichten für die Betreiber kritischer Infrastrukturen erweitert. Der MDR ist nicht Adressat dieses Gesetzes, gleichwohl betrachtet er die Gewährleistung der IT-Sicherheit und damit die Aufrechterhaltung der Sendefähigkeit als Bestandteil der Erfüllung seiner staatsvertraglichen Aufgaben. Die öffentlich-rechtlichen Rundfunkanstalten engagieren sich deshalb im Branchenarbeitskreis Medien des UP KRITIS, einer öffentlich-privaten Kooperation zum Schutz kritischer Infrastrukturen in Deutschland. Die Etablierung von Sicherheitsmaßnahmen zur Gefahrenabwehr und Stabilisierung von IT-Systemen wird immer wichtiger, gerade im Hinblick auf die in den letzten Jahren und Monaten spürbare Zunahme von Angriffen auf die IT-Systeme. Insofern müssen hier die Entwicklungen sowohl in tatsächlicher als auch rechtlicher Hinsicht aufmerksam beobachtet werden.

3.6. Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDGS)

Unter Ziffer 3.3 des letzten Berichtes habe ich über den Entwurf des TTDGS berichtet. Dieses Gesetz trat zum 1. Dezember 2021 in Kraft. Es beinhaltet Vorschriften zum Schutz des Fernmeldegeheimnisses, des Datenschutzes und bislang im Telemediengesetz enthaltene Regelungen. Der Gesetzgeber hat überdies beabsichtigt, Vorgaben aus der DSGVO und der e-Privacy-Richtlinie auszuformen bzw. umzusetzen.

Für den MDR von großer Bedeutung ist in der Praxis § 25 TTDSG, der den Schutz der Privatsphäre in Endgeräten regelt. Danach ist jedes Smartphone ebenso eine Endgeräts-Einrichtung wie jeder Laptop, jedes Tablet oder jeder PC, der direkt mit dem Internet verbunden ist.

Nach § 25 TTDSG ist die Speicherung von Informationen in diesen Endgeräten der Nutzer oder der Zugriff auf Informationen, die bereits dort gespeichert sind, in der Regel nur zulässig, wenn die/der Endnutzer/-in hierin eingewilligt hat. § 25 Abs. 2 TTDSG formuliert jedoch auch Ausnahmen. Wichtig für den MDR ist die Ausnahme, wonach es keiner Einwilligung bedarf, wenn der Zugriff auf die oder die Speicherung der Information im Endgerät unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes ein vom Nutzer/-in ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Für den MDR gilt: Beim Einsatz von Cookies, Local Storage Elementen, Identifiern und vergleichbaren Technologien in den Telemedienangeboten muss in jedem Einzelfall geprüft werden, ob das Cookies oder das andere Element für die Zurverfügungstellung des Dienstes unbedingt erforderlich ist. Zulässig ist es deshalb bspw. die bevorzugte Sprache für die Kommunikation zu speichern, nicht aber Marketing-Cookies oder solche zur personalisierten Reichweitenmessung. Das Gesetz ist erst Ende des Jahres 2021 in Kraft getreten, sodass es noch keine Rechtsprechung zu der Frage gibt, was als unbedingt erforderlich angesehen werden kann. Auch die RDSK befasst sich aktuell mit dieser Frage in Bezug auf die von ihr beaufsichtigten öffentlich-rechtlichen Rundfunkanstalten und ebenso gibt es eine Orientierungshilfe der staatlichen Aufsichtsbehörden für die Anbieter:innen von Telemedien ab dem 01.12.2021 (siehe hierzu auch Kapitel 4.6).

3.7. Urteil des OVG Schleswig-Holstein vom 25.11.2021 zur Untersagung des Betriebs einer Facebook-Fanpage

Im Tätigkeitsbericht für den Zeitraum der Jahre 2018 - 2019 hatte ich über die Verantwortung für Fanpages bei Facebook berichtet (Kapitel 4.1). Der EuGH hat im Wesentlichen bereits 2018 entschieden, dass Fanpage-Betreiber gemeinsam mit Facebook Verantwortung tragen für die dort stattfindende Datenverarbeitung. Der EuGH hat festgestellt, dass die Akteurinnen und Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und unterschiedlichen Ausmaß in der Weise einbezogen sein können, dass der Grad der Verantwortlichkeit eines jeden unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist. Daraufhin hat das Bundesverwaltungsgericht am 11.09.2019 die Entscheidung des EuGH bestätigt und die Sache an das Oberverwaltungsgericht (OVG) Schleswig-Holstein zurückverwiesen. Das OVG Schleswig-Holstein kommt in seiner ausführlichen Urteilsbegründung u.a. zu dem Schluss, dass bereits die Einrichtung einer Fanpage auf Facebook von Seiten ihres Betreibers und der damit verbundenen Auswahl der dort platzierten Inhalte ein bestimmtes Zielpublikum anzieht, was sich auf die Verarbeitung personenbezogener Daten zum Zweck der Erstellung von Statistiken auswirkt. Mit anderen Worten: Bereits die Charakteristik der Fanpage führt dazu, dass nur ein bestimmtes Zielpublikum angesprochen und damit die Auswahl der Daten, die dort verarbeitet werden, beeinflusst wird. Mit dieser sehr weiten Auslegung der Verantwortlichkeit geht das Gericht noch einen Schritt weiter und erkennt in jedem Fall bei der Präsenz auf Drittplattformen eine gemeinsame Verantwortlichkeit. Insofern müssen die Anstalten zukünftig sehr genau prüfen, welchen Grad der Verantwortung sie treffen könnte und sind daher verpflichtet, ggf. Joint-Controller-Verträge mit den Drittplattformen abzuschließen – was sich als überaus schwierig erweisen könnte.

4. Datenschutz beim MDR

4.1. Neue Standardvertragsklauseln

Unter Punkt 9.3 des vergangenen Tätigkeitsberichtes hatte ich über ein Urteil des EuGH berichtet, das immense Auswirkung auf die Datenübermittlung in Drittländer hatte und noch hat. Der EuGH ist zum Schluss gekommen, dass das EU-US-Datenschutzabkommen (privacy shield) den datenschutzrechtlichen Anforderungen nicht genügt und somit andere Maßnahmen ergriffen werden müssen, damit die Datenübermittlung z. B. in die USA rechtmäßig ist. Ich hatte über diesbezügliche Empfehlungen der RDSK berichtet und gleichzeitig erläutert, dass die EU-Standardvertragsklauseln weiterhin gültig sind.

Im Berichtsjahr kam nun eine Neuerung hinzu: Die EU-Kommission hat im Nachgang zum sogenannten „Schrems II“ Urteil des EuGH, die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer neu gefasst (siehe dazu auch 3.3 dieses Berichtes). Dabei handelt es sich um Vertragsklauseln im Sinne geeigneter Garantien nach Artikel 46 DSGVO, die dann zur Anwendung kommen können, wenn kein sogenannter Angemessenheitsbeschluss der EU-Kommission in Bezug auf die Datenverarbeitung im jeweiligen Drittland vorliegt. Mit anderen Worten: Hat die EU-Kommission ein geeignetes Datenschutzniveau in einem Drittland nicht festgestellt (wie bspw. in den USA), so sind diese Standardvertragsklauseln anzuwenden. Wichtig ist, dass diese Vertragsklauseln unverändert verwendet werden müssen und ggf. durch zusätzliche Sicherheitsmaßnahmen flankiert werden.

Die aktualisierten Standardvertragsklauseln haben einen recht komplizierten modularen Aufbau, aus denen sich die Verwendenden den passenden Vertrag „zusammenbauen“ müssen. Um eine einheitliche Handhabung auch auf ARD/ZDF-Ebene zu ermöglichen, sind beim MDR die einzelnen Module auseinandergenommen und für den jeweils passenden Zweck bearbeitet worden. Damit konnten Vertragsmuster hergestellt werden, die die Verwendung dieser Standarddatenschutzklauseln vereinfachen. Insgesamt ist ein Beitrag zur sicheren Datenübermittlung in Drittstaaten geleistet worden.

4.2. Kontrolle des Arbeitgebers des 3G-Status

Auch im Jahr 2021 waren datenschutzrechtliche Probleme im Zusammenhang mit der Coronapandemie zu lösen. Schlussendlich hat es im Herbst 2021 eine Änderung des Infektionsschutzgesetzes gegeben, nach dem Arbeitsstätten nur mit einem Impfnachweis oder einem Genesenen-Nachweis betreten werden durften. Die Arbeitgeber waren überdies verpflichtet, dies zu überwachen und auch zu dokumentieren. Hier stellte sich die Frage, wie dies datenschutzgerecht umzusetzen war.

Wichtig ist immer, gerade bei Gesundheitsdaten, dass möglichst datensparsam agiert wird. Es ist also immer schwierig, Gesundheitsdaten, die auch Personen direkt zugeordnet werden können, langfristig aufzubewahren. Im vorliegenden Fall war es ja nur nötig, den Impfstatus einmal zur Kenntnis zu nehmen und zu vermerken. Es wurde die Lösung gefunden, die Transponder dementsprechend zu programmieren und eine elektronische Einlasskontrolle durchzuführen. Somit ist der Impfstatus zwar vermerkt, ein Zugriff jedoch nur begrenzt möglich. Der Genesenenstatus für ungeimpfte Mitarbeiterinnen und Mitarbeiter kann direkt an der Wache durch die entsprechende Einsichtnahme sichergestellt werden. Insgesamt ein datenschutzrechtlich immer wieder schwieriges Thema, das aber beim MDR gesetzeskonform umgesetzt worden ist.

4.3. Interaktives Hörspiel

Innovation wird groß geschrieben. MDR Next plante im Berichtsjahr ein interaktives Hörspiel, das via MDR Website und Amazon Alexa ausgespielt werden sollte. Laut Projekt sollen die Zuhörerinnen und Zuhörer selbst eine Hauptrolle übernehmen, sie entscheiden, wie die Geschichte weitergeht und können insofern direkt mitgestalten.

Aus Datenschutzsicht war interessant, wie die Datenverarbeitung stattfindet. Zunächst einmal findet eine Interaktion zwischen dem Smart Speaker und der jeweiligen Nutzerin oder dem Nutzer statt. Dieses Verhältnis betrifft den MDR nicht direkt. Auskunftsgemäß werden die Spracheingaben dort (bei Amazon) transkribiert

und anonymisiert und an das Backend des MDR bzw. seines beauftragten Dienstleisters weitergegeben, wo dann die entsprechende Auswahl ausgelöst wird. Diese Verbindung ist laut Auskunft sowohl von Amazon als auch vom Dienstleister über eine anonymisierte ID abgesichert. Insofern können keine Rückschlüsse auf die einzelnen Nutzerinnen und Nutzer gezogen werden. Insgesamt scheint aber das datenschutzrechtliche Risiko auch deswegen vertretbar, weil keine Klarnamen verwendet werden und auch die Sprachdaten nicht übermittelt werden. Insgesamt ist das redaktionelle Angebot auch durch das Medienprivileg datenschutzrechtlich weniger streng zu betrachten.

Das Angebot eines interaktiven Hörspiels kann allerdings auch ohne Alexa wahrgenommen werden. Man kann sich also ohne Sprachassistenten in das interaktive Hörspiel einschalten. Hier findet ein Datenfluss direkt zu dem vom MDR beauftragten Dienstleister statt, sodass es eines sogenannten Auftragsverarbeitungsvertrages bedurfte. Denn für diese Datenverarbeitung ist der MDR unmittelbar verantwortlich. Mit Abschluss eines solchen Vertrages ist aber auch diese Datenverarbeitung rechtlich in Ordnung.

4.4. Einsatz von MS Teams

Ebenso pandemiegetrieben haben sich die Entwicklungen auf dem Gebiet der Kollaborationstools immens beschleunigt. Beim MDR war zunächst das Tool Circuit eingesetzt worden, im Zuge der ARD-Angleichung ergab sich die Notwendigkeit, sich mit dem Einsatz des Microsoft-Tools Teams auseinanderzusetzen. Hier stellten sich natürlich zahlreiche datenschutzrechtliche Fragen, sodass ich mich im Rahmen meiner Aufsichtstätigkeit entschlossen habe, an der Arbeitsgruppe zur Einführung mitzuwirken.

Bei einem solchen Projekt müssen insbesondere die Datenflüsse und die Datenarten, die dort verarbeitet werden, genau in den Blick genommen werden. Für jede Datenart und die damit zusammenhängende Datenverarbeitung muss geklärt werden, ob und ggf. welche Rechtsgrundlage einschlägig sein kann. Dann gibt es zusätzlich das Problem, dass Daten möglicherweise nicht in Europa, sondern auch in

den Vereinigten Staaten von Amerika verarbeitet werden. Auch gibt es nicht nur reine Nutzerdaten, sondern auch sogenannte Metadaten oder auch Telemetriedaten, die den eigentlichen Kommunikationsprozess unterstützen.

Unter all diesen Gesichtspunkten wurde die Datenverarbeitung bei MS Teams unter die Lupe genommen und schwerpunktmäßig eine Risikoanalyse durchgeführt. Dies entspricht der Wertung der Datenschutzgrundverordnung.

Insoweit konnte nach mehreren Sitzungen ein Datenschutzkonzept entwickelt und verabschiedet werden, dass alle datenschutzrechtlichen und auch IT-sicherheitsrelevanten Aspekte berücksichtigt und einen rechtssicheren Betrieb von MS-Teams ermöglicht. Selbstverständlich ist gerade bei diesen sehr komplexen Softwareprodukten stets aufmerksam zu verfolgen, ob und ggf. in welcher Weise sich die Datenverarbeitungsprozesse ändern und seitens des mächtigen Anbieters (hier Microsoft) abgeändert werden. In Zukunft soll MS 365 beim MDR eingeführt werden; auch hier ist in enger Zusammenarbeit mit allen anderen ARD-Anstalten genau zu prüfen, wie den datenschutzrechtlichen Risiken und Unwägbarkeiten begegnet werden kann. Ein Clouddienst, der auch sensible Daten der Rundfunkanstalten verarbeiten kann, muss besondere Sicherheitsmerkmale aufweisen. Wenn dies nicht so ist, ist damit auch die Integrität des öffentlich-rechtlichen Rundfunks in dieser Hinsicht gefährdet; dies muss unbedingt vermieden werden.

4.5. Auslagerung und Beratung zur Pensionskasse

Zukünftig wird die betriebliche Altersversorgung für die freien Mitarbeitenden des MDR von der Pensionskasse Rundfunk übernommen. Der MDR hat entschieden, die Beratung zur betrieblichen Altersversorgung ab dem 01.01.2022 an die Pensionskasse Rundfunk auszulagern. Es war zu klären, ob die Weitergabe der Daten und, wenn ja, unter welchen Voraussetzungen, datenschutzrechtlich statthaft ist.

Zunächst wurde festgestellt, dass die Beratung der freien Mitarbeitenden zu ihrer Altersversorgung eine Aufgabe des MDR ist. Damit wäre eine Beratung unmittelbar durch den MDR rechtlich einwandfrei und eine dementsprechende Datennutzung

gerechtfertigt. Heißt dies ebenso, dass diese Daten dann zum Zwecke der Beratung an die Pensionskasse Rundfunk weitergereicht werden können? Und bedeutet dies ggf., dass die Pensionskasse Rundfunk diese Daten auch zum Zweck des Vertragsabschlusses nutzen kann?

Hier war klar zu trennen: die Beratungsleistung als solche einerseits und der ggf. darauffolgende Vertragsabschluss zur betrieblichen Altersversorgung andererseits. Der MDR kann die Daten nur zur Beratung nutzen; will er diese Beratung nicht selbst übernehmen und damit einen Dritten beauftragen, so muss ein entsprechender Auftragsverarbeitungsvertrag geschlossen werden. Im vorliegenden Fall war darauf zu achten, dass sich die Datennutzung allein auf die Beratungsleistung beschränkt. Sollte die oder der der betreffende freie Mitarbeitende überzeugt sein und mit der Pensionskasse Rundfunk ins Geschäft kommen, dürfen die Daten, die der MDR übermittelt hat, dazu nicht verwendet werden. Es ist dann ein anderes Rechtsverhältnis maßgeblich, das auch anderen Regeln und anderen Rechtsgrundlagen folgt. Daher war in dem Vertrag zwischen MDR und der Pensionskasse Rundfunk sehr deutlich auf die strenge Zweckbindung der Daten hinzuweisen und klarzustellen, dass jede weitere Datenverwendung ausgeschlossen und ein Vertragsabschluss allein auf Grundlage einer neuen Datenerhebung mit den betroffenen Mitarbeitenden statthaft ist.

4.6. Mal wieder: Cookies

In Kapitel 3.6 berichte ich über das TTDSG. Dort habe ich angemerkt, dass in diesem Gesetz nicht nur das Datenschutzrecht betroffen ist, sondern auch die Integrität des Endgerätes als Schutzgut gilt. Daher musste sich der MDR mit der Frage auseinandersetzen, welche Informationen in der Endeinrichtung des Endnutzers bei seinen Angeboten gespeichert werden. Dazu gehören z. B. Cookies oder sogenannte Local Storage Elemente. Gemeinsam mit den Verantwortlichen wurde daher untersucht, welche Praxis beim MDR verfolgt wird.

Von einer Einwilligung zur Speicherung solcher Informationen auf den Endgeräten kann nur dann abgesehen werden, wenn dies unbedingt erforderlich ist, damit der

Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann. Hierzu gehören gewiss die Funktionalitäten des Telemediendienstes als solchen. Dazu gehören aber auch Cookies, die eine technische Fehleranalyse ermöglichen, der Sicherheit des Angebots dienen, Login-Daten seiner Nutzerinnen und Nutzer zur besseren Funktionalität speichern, sowie zur Individualisierung der Website-Inhalte (z. B. Schriftgröße) erforderlich sind.

Knackpunkt ist wie immer die Nutzungsmessung. Im öffentlich-rechtlichen Rundfunk – dies wird von den Rundfunkdatenschutzbeauftragten einhellig vertreten – braucht es für eine anonyme Nutzungsmessung keine Einwilligung. Dies, weil diese Messung dem verfassungsrechtlichen Funktionsauftrag dient, auf dessen Grundlage die Rundfunkanstalten die Bevölkerung mit einem auftragsgemäßen und publizistisch relevanten Angebot zu versorgen haben. Dies ergibt sich ebenso aus § 30 Abs. 3 Medienstaatsvertrags, nach dem es zum Auftrag gehört, zeitgemäß gestaltete Telemedienangebote anzubieten. Die Anstalten sind darauf angewiesen zu wissen, wie ihre digitalen Angebote wahrgenommen und genutzt werden. Mit anderen Worten: Was interessiert die Nutzerinnen und Nutzer? Zu berücksichtigen ist hier aber, dass sie dafür ausschließlich anonymisierte bzw. pseudonymisierte Daten auswerten lassen, so dass sie technisch schon nicht in der Lage sind, personenbezogene Nutzungsprofile anzulegen und auszuwerten. Dies ist wiederum der datenschutzrechtliche Aspekt an der Nutzungsmessung, der beim TTDSG – wie oben angeklungen – nicht im Vordergrund steht.

Es ist besonders wichtig, die Nutzerinnen und Nutzer im Rahmen von Datenschutzerklärungen über diese Besonderheit zu informieren, denn oftmals wird mit Erstaunen festgestellt, dass keine Einwilligungen zur Nutzungsmessung eingeholt werden. Es ist klar und verständlich über den Auftrag und die sich daraus ergebenden Besonderheiten aufzuklären und in verständlicher Weise die Ausnahme vom Einwilligungserfordernis darzulegen.

5. Datenschutz beim KiKA

5.1. Zusammenarbeit mit dem KiKA

Der betriebliche Datenschutz beim Kinderkanal, einer Gemeinschaftseinrichtung von ARD und ZDF, obliegt der federführenden Anstalt, hier also dem MDR. Herr Matthias Meincke ist als betrieblicher Datenschutzbeauftragter des MDR auch für den Datenschutz beim KiKA zuständig. Den Datenschutz vor Ort besorgt Herr Jörn Voss, der seit vielen Jahren dieses Amt innehat und in bewährter Weise die datenschutzrechtlichen Belange betreut und als Schnittstelle zwischen dem betrieblichen Datenschutzbeauftragten und auch dem Rundfunkdatenschutzbeauftragten fungiert.

Wie bisher in jedem Datenschutzbericht bekräftigt, funktioniert die Zusammenarbeit mit Herrn Voss in vorbildlicher Art und Weise: bereits frühzeitig und immer fachlich fundiert werden die datenschutzrechtlich problematischen Fälle aufbereitet und an den zuständigen Datenschutz beim MDR weitergeleitet. Das Engagement von Herrn Voss soll an dieser Stelle ausdrücklich gewürdigt werden. Herr Voss erstellt jedes Jahr eine Übersicht über seine Tätigkeiten. Seinen Jahresbericht 2021 ist diesem Tätigkeitsbericht als Anlage beigefügt.

5.2. KiKA Quiz-APP

Beim KiKA wird eine Quiz-App entwickelt. Wie immer besteht die datenschutzrechtliche Schwierigkeit darin, Kinderdaten rechtssicher so zu verarbeiten, dass die Risiken minimiert werden. Bei dieser Quiz-App sollen, um Spielstände und Aktivitäten speichern zu können, ein Spielname und ein Avatar ausgesucht werden. Es wird also ein Nutzungsprofil angelegt.

In der Diskussion wurde schnell klar, dass auf Klarnamen und sonstiges persönliche Daten von Kindern strikt verzichtet werden soll, da der KiKA auch kein Interesse daran hat. Um mitspielen zu können, muss jedoch ein Spielname und ein Avatar ausgewählt werden, um den Kindern die Möglichkeit zu geben, sich mit anderen

Mitspielenden zu messen und langfristig Spaß an der Applikation zu haben. Es werden also keine Personendaten wie Name, Alter oder die Anschrift verarbeitet. Es geht lediglich um eine Unterscheidbarkeit und um die Speicherung der Spielstände.

Digitale Spuren werden beim Nutzen einer App oder auch des Internets stets hinterlassen – zumindest die IP-Adresse und verschiedene Log-Daten fallen immer an. Eine Einwilligung in eine solche grundlegende Datenverarbeitung ist nicht notwendig, denn diese App kann technisch nicht anders betrieben werden. Gleiches gilt in diesem Fall auch für die Speicherung der Spielstände und des Avatars, denn nur so kann bei diesem Spiel in vorgesehener und sinnvoller Weise mitgemacht werden.

Die Besonderheit in diesem Fall ist jedoch, dass die Adressaten Kinder sind. Daher hat sich das Entwicklerteam gemeinsam mit den Datenschutzbeauftragten von MDR und KiKA darauf geeinigt, dass aus pädagogischen Gründen beim Start-Screen die Kinder aufgefordert werden, die Eltern einzubeziehen und sie mitentscheiden zu lassen, ob ein solcher Avatar und Nickname ausgewählt wird. Obwohl das in diesem Fall aus streng rechtlichen Gründen nicht unbedingt erforderlich gewesen wäre, schien es allen Beteiligten besser, die Eltern einzubinden. Die Kinder sollen auch vom KiKA – einem absolut sicheren Umfeld – nicht das Gefühl vermittelt bekommen, dass man im Umgang mit digitalen Medien und Applikation sorglos sein darf.

5.3. Datenschutzvorfall Presselounge

Der KiKA betreibt eine Presselounge. Dort können angemeldete Nutzerinnen und Nutzer spezielle Presseinformationen abrufen. Während eines kurzen Zeitraums im Januar 2021 hat die Möglichkeit bestanden, ein Profil einer anderen Person durch nicht autorisierte Nutzende einzusehen. In diese Zeitspanne haben insgesamt 20 Nutzende auf die Presselounge zugegriffen (dies war an 20 IP-Adressen zu erkennen); es ist nicht nachvollziehbar, ob diese Besuche auch zu einer tatsächlichen Offenlegung von Daten geführt haben. Mir wurde mitgeteilt, dass durch Umbaumaßnahmen Daten versehentlich an einer falschen Stelle gespeichert worden seien.

Durch technische Vorkehrungen wird künftig dafür gesorgt, dass dies nicht mehr vorkommen kann.

Dieser Vorfall ist mir im Rahmen einer Meldung gemäß Artikel 33 DSGVO zu Kenntnis gebracht worden. Ich hatte daher zu prüfen, ob ein erhöhtes Risiko für die Rechte und Freiheiten natürlicher Personen zu befürchten sind. Ein Risiko besteht u. a. darin, wenn den betroffenen Personen – im vorliegenden Fall lediglich einer Person – Diskriminierung, Identitätsdiebstahl, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von Berufsgeheimnissen oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen.

Eine genaue Untersuchung hat ergeben, dass ein erhebliches Risiko für die eine Person nicht bestanden hat. Die Daten der dort registrierten Nutzerinnen und Nutzer bewegen sich im beruflichen Kontext. Sie unterliegen keiner besonders geschützten Vertraulichkeit. Ein Bekanntwerden dieser Daten führt zu keinen erkennbaren Risiken bei den betroffenen Personen in der beschriebenen Art.

Ich habe empfohlen, die betroffene Person über die technische Fehlfunktion der KiKA Presselounge zu informieren und ihr ggf. anzuraten, das Profil neu anzulegen und mit einem neuen Passwort zu versehen. Insgesamt wurde auch noch einmal darauf hingewirkt, die beteiligten Bereiche für solcherlei Vorfälle zu sensibilisieren und in Zukunft mehr Sorgfalt walten zu lassen.

6. Datenschutz beim Zentralen Beitragsservice

6.1. Datenschutz im Zusammenhang mit dem Rundfunkbeitrag

Die Daten der Rundfunkbeitragszahler werden zentral verwaltet durch den ARD, ZDF und Deutschlandradio Beitragsservice. Rechtsangelegenheiten sowie Klagen gegen den Beitragsservice werden dagegen dezentral von den einzelnen Rundfunkanstalten betreut.

Für die Kontrolle des Zentralen Beitragsservice sind die Datenschutzbeauftragten der einzelnen Rundfunkanstalten jeweils für ihren Teilnehmerkreis nach Maßgabe des für die Rundfunkanstalt geltenden Rechts zuständig. Die Ausnahme bilden auch hier die Länder Berlin und Brandenburg beim rbb, Bremen bei Radio Bremen und Hessen für den Hessischen Rundfunk. Hier üben die Landesdatenschutzbeauftragten die Kontrollfunktion aus. Dieser geteilten Zuständigkeit begegnen verfassungsrechtliche Bedenken, gerade im Hinblick auf die Staatsferne des Rundfunks. Durch die Einbindung der Landesdatenschutzbeauftragten wird eine staatliche Kontrolle vorgesehen, die insbesondere den verfassungsrechtlich sensiblen geschützten Bereich der Rundfunkfinanzierung betrifft.

Beim Zentralen Beitragsservice ist eine behördliche Datenschutzbeauftragte mit den täglichen Aufgaben betraut und dort verantwortlich für die Organisation des Datenschutzes. Mit ihr und ihrem Stellvertreter habe ich häufig Kontakt, denn sobald mich Beschwerden erreichen, die den Rundfunkbeitragseinzug und die damit zusammenhängende Datenverarbeitung betreffen, muss ich mich an den Beitragsservice für eine Stellungnahme wenden. Die Zusammenarbeit verläuft reibungslos und soll an dieser Stelle ausdrücklich gewürdigt werden.

Die Beitragszahler-Daten und die Behandlung datenschutzrechtlicher Fragen in diesem Zusammenhang beschäftigen den AK DSB wie gewohnt häufig. Im Berichtsjahr wurden insbesondere weitere Fragen zur Löschung dieser Daten und Konten diskutiert und besprochen. In alle Fragen rund um den Datenschutz werden sowohl die betrieblichen Datenschutzbeauftragten der Rundfunkanstalten als auch die Rundfunkdatenschutzbeauftragten in ihrer Aufsichtsfunktion einbezogen.

6.2. Umsetzung des Löschkonzeptes

Das Datenverarbeitungssystem des Zentralen Beitragsservices besteht schon seit vielen Jahren und beinhaltet verschiedene Altdaten, deren Löschung sich über die Jahre als schwierig erwiesen hat, da aufgrund der schieren Masse und der technischen Abhängigkeiten kritische Folgen befürchtet wurden. Die Stabilität des Beitragseinzugs und die Integrität des Systems standen insoweit im Vordergrund. Deshalb wurden große Anstrengungen unternommen, auch Altdaten, die nur aus Sicherheitsgründen im System verblieben sind, restlos zu löschen. So mussten über die Jahre sukzessive veraltete Daten gelöscht werden, z. B. Stamm- und Korrespondenzanschriften, Befreiungsdaten, Mahnmaßnahmen und Buchungsbelege. Im November 2021 konnte vom Zentralen Beitragsservice vermeldet werden, dass die Umsetzung des Löschkonzeptes erfolgreich abgeschlossen ist. Der AK DSB hat an der Erstellung des Löschkonzeptes und der Umsetzung mitgewirkt und den Prozess unterstützend begleitet.

7. Datenschutz im IVZ

7.1. Datenschutz im Informationsverarbeitungszentrum (IVZ)

Beim IVZ, der Gemeinschaftseinrichtung der ARD Anstalten und des Deutschlandradios werden u. a. alle Personal- und Archivdaten für die Rundfunkanstalten verarbeitet. Das IVZ unterstützt die Häuser in den Bereichen SAP, Archiv- und Produktionssysteme, IT-Support sowie Rechenzentrumsleistungen. Überdies übernimmt das IVZ die Steuerung der Vereinheitlichung der SAP-Prozesse für den öffentlich-rechtlichen Rundfunk.

Neben dem einmal jährlich stattfindenden Treffen „IT-Sicherheit und Datenschutz“ beim IVZ gab es im Berichtsjahr einen zusätzlichen Austausch zwischen IVZ und AK DSB am 07.10.2021. Dort wurden die Fragen diskutiert, die sich aus der Verwaltungsvereinbarung über das IVZ sowie dem abgeschlossenen Joint-Control-

ler-Vertrag ergeben. Es wurde besprochen, wie der Datenschutz am besten umzusetzen ist und wie der Austausch zwischen der rbb-Datenschutzbeauftragten (dort örtlich zuständig) sowie dem Datenschutzbeauftragten des IVZ am besten organisiert wird. Ebenso wurde erörtert, wie mit Risiken umzugehen ist. In diesem Zusammenhang gab es überdies einen Austausch über die Datenschutzfolgenabschätzung zum Einsatz von Microsoft 365 beim IVZ.

Das jährliche Treffen IT-Sicherheit und Datenschutz im IVZ fand im Berichtsjahr am 02.12.2021 statt. Hier wurde über die Ergebnisse des Überwachungsaudits berichtet sowie der Datenschutzbericht des IVZ im Entwurf vorgestellt. Es wurden verschiedene Punkte mit den Datenschutzbeauftragten der Rundfunkanstalten diskutiert, im Ergebnis konnten die strittigen Punkte ausgeräumt und Arbeitsaufgaben verteilt werden.

Ein aktives Eingreifen im Sinne einer offiziellen Beanstandung war bei der Datenverarbeitung des IVZ im Berichtsjahr nicht notwendig.

8. Datenschutz bei Tochterfirmen des MDR

8.1. Datenschutzvorfall bei der AVI.DAT Software und Technologie GmbH

Im Herbst 2021 erreichte mich eine Meldung des betrieblichen Datenschutzbeauftragten der AVI.DAT GmbH. Die AVI.DAT ist eine 100%ige Tochterfirma der MDR Media GmbH, die wiederum eine 100%ige Tochter des MDR ist. Somit fungiere ich auch bei diesem Tochterunternehmen als Aufsichtsbehörde.

Die AVI.DAT wollte über ein Produkt-Update einer Software unterrichten, die die Firma entwickelt und verkauft. Die Empfänger, in diesem Fall die Betroffenen, wurden versehentlich per Carbon Copie (CC per Mail) und nicht per Blind Carbon Copie (BCC) angeschrieben. Dadurch war es den angeschriebenen Personen möglich, auf

personenbezogene Daten zuzugreifen, die ihren Augen eigentlich hätten verborgen bleiben müssen. Insofern handelt es sich hierbei um eine unzulässige Offenlegung von Daten.

Es kann natürlich einmal passieren, dass man aus Unachtsamkeit die Mails falsch verschickt. Im vorliegenden Fall waren auskunftsgemäß 33 Personen betroffen, die Frage war nun, wie angemessen auf einen solchen Vorfall reagiert werden muss.

Die AVI.DAT hat zunächst richtig gehandelt, in dem sie den Vorfall gemäß Artikel 33 DSGVO der zuständigen Aufsichtsbehörde gemeldet hat. Ebenso wurden die betroffenen Personen unverzüglich von der Verletzung unterrichtet. Dies ist zwar gemäß Artikel 34 DSGVO ausschließlich dann erforderlich, wenn die Verletzung des Schutzes der personenbezogenen Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Personen zur Folge hat, jedoch stand hier das grundsätzliche Risiko eines Identitätsdiebstahls im Raum, sodass die betroffenen Personen von dem Fehler unterrichtet werden sollten. In Anbetracht der Tatsache, dass es sich um 33 Betroffene handelte, war der Aufwand auch überschaubar und daher gut vertretbar.

Der betriebliche Datenschutzbeauftragte hat richtigerweise darauf hingewiesen, dass es sich in diesem Fall um menschliches Versagen handelte, sodass technische Maßnahmen zur Verhinderung zukünftiger Datenschutzverletzungen nicht im Raum standen. Insgesamt wurden Schulungsmaßnahmen angekündigt, um die Mitarbeiterinnen und Mitarbeiter der AVI.DAT zu sensibilisieren und künftiges Fehlverhalten möglichst auszuschließen. Ebenso wurde geprüft, ob eine technische Unterstützung zur Vermeidung solcher Fehler denkbar ist.

Aufgrund der schnellen Reaktion der AVI.DAT sowie der nur geringen Schwere des Datenschutzverstoßes habe ich von weiteren aufsichtsrechtlichen Maßnahmen abgesehen. Eine spätere Kontrolle der eingeleiteten Maßnahme bleibt jedoch vorbehalten.

9. Rundfunkdatenschutzkonferenz (RDSK)

9.1. Grundsätzliches

Die Rundfunkdatenschutzkonferenz (RDSK) ist der Zusammenschluss der Rundfunkdatenschutzbeauftragten. Die RDSK besteht unverändert aus acht Personen, die die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk über die Rundfunkanstalten und deren Gemeinschaftseinrichtungen und Beteiligungsunternehmen ausüben. Die Mitglieder der RDSK blieben unverändert (siehe Liste der Mitglieder der RDSK im Anhang).

Im Berichtsjahr hat den Vorsitz der Rundfunkdatenschutzbeauftragte des Bayerischen Rundfunks, des Saarländischen Rundfunks, des Westdeutschen Rundfunks, des Deutschlandradios und des Zweiten Deutschen Fernsehens, Herr Dr. Reinhart Binder übernommen. Stellvertreterin war die Datenschutzbeauftragte des Rundfunks Berlin Brandenburg, Frau Anke Naujock-Simon.

9.2. Funktion der RDSK

Die Aufgaben der RDSK ergeben sich aus der Geschäftsordnung, die sich die RDSK 2019 gegeben hat.

Die RDSK soll einen Beitrag zur einheitlichen Anwendung der DSGVO leisten, insbesondere soweit es um die Anwendung im öffentlich-rechtlichen Rundfunk geht. Die Mitglieder arbeiten unter Wahrung der jeweiligen Unabhängigkeit eng zusammen und tauschen sich aus. Neben der Geschäftsordnung gibt es zwei Verwaltungsvereinbarungen. Einmal zur Wahrnehmung der Datenschutzaufsicht über die Gemeinschaftsunternehmen der Rundfunkanstalten und zweitens zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten. Hier sind die Zuständigkeiten der RDSK niedergelegt. Seit Beginn des Jahres 2020 können diese Dokumente auf der Homepage der RDSK abgerufen werden:

www.rundfunkdatenschutzkonferenz.de

Dort finden sich auch die Veröffentlichungen der RDSK, von denen es zwei neue im Berichtsjahr gab: Einmal eine Entschließung der RDSK zu der App Clubhouse sowie die Eckpunkte zum Einsatz von Kollaborationssystemen.

Die RDSK hat im Jahr 2021 zu einer Sitzung zusammengefunden. Schwerpunkte dieser Sitzung sowie des sonstigen Austausches waren:

- Das Verfahren der Zusammenarbeit mit den Aufsichtsbehörden des Bundes und der Länder nach § 18 Absatz 1 Satz 4 BDSG,
- die Nutzung von Drittplattformen durch die Rundfunkanstalten,
- Aufsichtszuständigkeiten bei Kooperationen im Programmbereich,
- Anwendung von Artikel 83 DSGVO (Bußgeldrahmen),
- Umsetzung von Artikel 35 Absatz 4 DSGVO („Blacklist“ für eine Datenschutzfolgenabschätzung),
- die Auswirkungen des TTDSG auf die Telemedienangebote der Rundfunkanstalten,
- Einsatz der Luca App.

Die RDSK hat im Rahmen einer Abfrage der EU-Kommission zur Umsetzung der DSGVO auf nationaler Ebene Stellung genommen und den Evaluierungsprozess begleitet.

Im Mai und Dezember 2021 fanden Sitzungen mit der Datenschutzkonferenz (DSK), dem Gremium der Datenschutzaufsichtsbehörden des Bundes und der Länder statt. In diesen regelmäßig stattfindenden Runden, an dem u. a. auch die Aufsichtsbehörden der Kirchen teilnehmen, werden regelmäßig aktuelle Themen besprochen. Dazu gehören u.a. aktuelle Entwicklungen im europäischen Datenschutz, Berichte über die Tätigkeitsschwerpunkte der Aufsichtsbehörden, die Evaluation des Bundesdatenschutzgesetzes, Kollaborationssysteme und das TTDSG.

Mitglieder der RDSK nehmen zudem an Sitzungen der Arbeitskreise Medien, Grundsatz und Technik der DSK teil. Ziel ist es, den Kontakt zu intensivieren, Wissen auszutauschen und die Positionen des Rundfunks auch auf dieser Ebene zu vertreten.

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

10.1. Zusammenarbeit im AK DSB

Neben der RDSK besteht der AK DSB als Gremium der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten. Hier treffen sich sowohl die Rundfunkdatenschutzbeauftragten als auch die internen oder betrieblichen Datenschutzbeauftragten, um sich zu Fragen des Datenschutzes auszutauschen. Es hat sich aus meiner Sicht nach wie vor bewährt, dass hier ungeachtet der speziellen Funktion der Mitglieder des AK DSB über rundfunkspezifische Themen diskutiert wird und ein Wissens- und Ideentransfer stattfindet. Ich habe es in den vergangenen Berichten oft bekräftigt: die Schnittmengen der Themen sind vielfältig und werden zwischen betrieblichem Datenschutz und den Aufsichten in diesem Gremium für alle Seiten bereichernd besprochen.

Der AK DSB tagt nach wie vor zweimal pro Jahr. Ergänzt werden diese Sitzungen durch alle zwei Monate stattfindende Videokonferenzen, die aktuell Wichtiges und den direkten Austausch über die Arbeit zum Inhalt haben. Die Zunahme an Themen, das Erfordernis nach zügigen Entscheidungen und der erhöhte Abstimmungsbedarf durch gemeinsame Vorhaben der Rundfunkanstalten sind Gründe für diesen intensivierten Austausch.

Zudem hat sich der AK DSB nunmehr eine Geschäftsordnung gegeben. Vorsitzender des AK DSB war im Berichtsjahr nach wie vor Herr Dr. Heiko Neuhoff vom Norddeutschen Rundfunk. Als solcher war er verantwortlich für die Erstellung der Tagesordnungen, die Einberufung der Sitzungen sowie die Leitung der Zusammenkünfte. Seine Stellvertretung habe ich übernommen.

Schwerpunktmäßig hat sich der AK DSB mit folgenden Themen befasst:

- Rundfunkteilnehmerdatenschutz
- Umsetzung des 23. Rundfunkänderungsstaatsvertrages beim Beitragsservice
- Übermittlung personenbezogener Daten in die USA

- Überarbeitung des Musters für eine Auftragsverarbeitungsvereinbarung
- Datenschutzrechtliche Begleitung der SAP-Harmonisierung
- Datenschutzfolgenabschätzung für Microsoft 365
- Zentrales SIEM/SOC für die ARD
- Überarbeitung der Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten
- Nutzungsmessung in Telemedienangeboten
- Joint-Controller-Vereinbarungen
- Neue Standardvertragsklauseln für Datenübermittlung in Drittländer
- Personalisierung von Mediatheken
- Kinderdatenschutz in Apps
- Datenschutzrechtliche Fragen zur Coronapandemie

Eine wichtige und zeitraubende Aufgabe war auch die Befassung mit unterschiedlichen Modulen des SAP-Systems im Zuge der Harmonisierungsbemühungen. Nach jetzigem Stand konnten die ehrgeizigen Ziele nicht eingehalten werden, sodass lediglich der Mitteldeutsche Rundfunk Anfang 2023 mit dem neuen System produktiv gehen wird. Hier ergaben sich verschiedene datenschutzrechtliche Fragen zur Nutzung von Echtdateien und den diesbezüglichen Zugriffsrechten, die die Datenschutzverantwortlichen des MDR stets im Auge zu behalten haben.

10.2. Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten der Rundfunkanstalten

Im Jahr 2016 hatte der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten der Rundfunkanstalten herausgegeben. Dieser Leitfaden sollte sich als Ratgeber an Mitarbeiterinnen und Mitarbeiter der Telemedien und Social-Media-Angebote der Rundfunkanstalten richten. Ziel war es, eine Orientierung zu bieten und den Verantwortlichen in den Anstalten dabei zu helfen, datenschutzrelevante Themen zu erkennen, zu beurteilen und sie mit datenschutzrechtlichen

Vorgaben verantwortungsvoll in Einklang zu bringen. Der Fokus lag dabei auf praxisrelevanten Einzelthemen von A wie Apps bis W wie Webanalyse.

Anfang des Jahres 2021 hat sich eine Arbeitsgruppe im AK DSB gebildet, die diese Leitlinien einer Grunderneuerung unterziehen wollte. Dies war deswegen notwendig geworden, weil sich einerseits die technischen Gegebenheiten, aber auch und vor allem die rechtlichen Rahmenbedingungen geändert haben. Eine Anpassung war deswegen unumgänglich, denn eine praxisorientierte Hilfestellung zu datenschutzrechtlichen Fragen auf diesem Gebiet ist von größter Wichtigkeit.

Das Reaktionsteam für diesen Leitfaden hat sich zusammengesetzt aus Kolleginnen und Kollegen des NDR, des RBB, des WDR, des HR, des Deutschlandradios und des MDR. Die Arbeit an den einzelnen Kapiteln ist aufgeteilt worden, sodass die Arbeit nicht nur auf wenigen Schultern ruhte. Insgesamt hat sich gezeigt, dass es sehr wichtig war, auch im gemeinsamen Austausch die Probleme und „Knackpunkte“ der einzelnen Themen zu identifizieren und in der gemeinsamen Diskussion so aufzubereiten, dass sie auch dem juristischen Laien verständlich vermittelt werden können und eine praktische Umsetzung in der täglichen Arbeit erleichtert wird.

Themen sind u.a. Hinweise zu einer korrekten Datenschutzerklärung, zu Cookies, zur Nutzungsmessung, zur Personalisierung, zu Drittplattformen sowie zum Minderjährigen-Datenschutz.

Angesichts der rasanten technischen und rechtlichen Entwicklung ist dieses Dokument als „lebend“ angelegt, damit kurzfristig auf Änderungen und Neuerung bspw. in der Rechtsprechung reagiert werden kann. Das Ziel, die Leitlinien bereits in Jahr 2021 zu veröffentlichen, ist nicht ganz erreicht worden. Der AK DSB hat die Leitlinien inhaltlich abgenommen und Anfang des Jahres 2022 veröffentlicht.

Die Leitlinien folgen der Zielsetzung des AK DSB, eng mit den Häusern und den Redaktionen zusammenzuarbeiten, um anwendungsorientiertes Wissen und entsprechende Hilfestellungen zu vermitteln. Wir hoffen, damit einen sinnvollen Beitrag geleistet zu haben.

11. Schlussbemerkungen

Das Spektrum an Themen und Problemen im Berichtsjahr 2021 war wie immer vielfältig und interessant. Es hat sich insbesondere gezeigt, dass eine Verlagerung der Datenverarbeitung außerhalb der eigenen Systeme und insbesondere in Drittländern nicht zu unterschätzen ist. Es ist schlicht nicht zu ignorieren, dass internationaler Datentransfer und die Verarbeitung bei Dienstleistern im außereuropäischen Ausland die Anstalten und auch alle sonstigen Akteure in Europa vor fast nicht zu bewältigende Schwierigkeiten stellt. Die Anforderungen an die Datensicherheit werden immer höher und die Komplexität der Probleme nimmt auch nicht ab. Daher ist es wichtig, dass die Rundfunkdatenschutzaufsichten und auch die internen Datenschutzbeauftragten eng zusammenarbeiten und gemeinsam mit den Anstalten Lösungen erarbeiten, die die Datenverarbeitung lediglich im europäischen Ausland und vielleicht auch auf eigenen Systemen in den Fokus rücken. Ebenso muss die rechtliche und politische Entwicklung in dieser Hinsicht genau beobachtet und ggf. Einfluss genommen werden.

Die Zusammenarbeit mit dem Verantwortlichen und dem betrieblichen Datenschutz des MDR hat auch in diesem Jahr bestens funktioniert. Ich bin guten Mutes, dass auch die kommenden Jahre mit ihren neuen und spannenden Herausforderungen gut zu bewältigen sein werden. Ich darf für das in mich gesetzte Vertrauen danken und freue mich auf die weitere Zusammenarbeit.

12. Anhang

Gesetzliche Grundlagen

12.1. MDR-Staatsvertrag (§§ 36 bis 40)

§ 36 Geltung von Datenschutzvorschriften

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

§ 37 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 haftet 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.

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.

§ 38 Ernennung des Rundfunkbeauftragten oder des Rundfunkbeauftragten für den Datenschutz beim MDR und der Datenschutzbeauftragten oder des Datenschutzbeauftragten des MDR

(1) Der MDR ernennt eine Rundfunkbeauftragte oder einen Rundfunkbeauftragten für den Datenschutz beim MDR (Rundfunkdatenschutzbeauftragte oder 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. Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, nachgewiesen durch ein abgeschlossenes Hochschulstudium, sowie über Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Das Amt der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten kann nicht neben anderen Aufgaben innerhalb des MDR und seiner Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten zu vereinbaren sein und dürfen ihre oder 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. Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte kann ihres oder seines Amtes nur enthoben werden, wenn sie oder er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Dies geschieht durch Beschluss des Rundfunkrates auf Vorschlag des Verwaltungsrates; die Rundfunkdatenschutzbeauftragte oder 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) Die Datenschutzbeauftragte oder der Datenschutzbeauftragte des MDR nach Artikel 37 der Verordnung (EU) 2016/679 wird von der Intendantin oder von dem Intendanten mit Zustimmung des Verwaltungsrates benannt.

§ 39 Unabhängigkeit der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten

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

(2) Die Dienststelle der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten wird bei der Geschäftsstelle von Rundfunkrat und Verwaltungsrat eingerichtet. Der Rundfunkdatenschutzbeauftragten oder dem Rundfunkdatenschutzbeauftragten ist die für die Erfüllung ihrer oder 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 der Rundfunkdatenschutzbeauftragten oder dem Rundfunkdatenschutzbeauftragten im Haushaltsvollzug zuzuweisen. Einer Finanzkontrolle durch den Verwaltungsrat unterliegt die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte nur insoweit, als ihre oder seine Unabhängigkeit bei der Ausübung ihres oder seines Amtes dadurch nicht beeinträchtigt wird.

(3) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte ist in der Wahl ihrer Mitarbeiterinnen oder seiner Mitarbeiter frei. Sie unterstehen allein ihrer oder seiner Leitung.

§ 40 Aufgaben und Befugnisse der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten

(1) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Datenschutzvorschriften dieses Staatsvertrages, des MStV, der Verordnung (EU) 2016/679 und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des MDR und seiner Beteiligungsunternehmen im Sinne des § 42 Absatz 3 Satz 1 MStV. Sie oder er hat die Aufgaben und Befugnisse entsprechend der Artikel 57 und 58 Absatz 1 bis 5 der Verordnung (EU) 2016/679. Bei der Zusammenarbeit mit anderen Aufsichtsbehörden hat sie oder er, soweit die Datenverarbeitung zu journalistischen Zwecken betroffen ist, den Schutz von Informanten zu wahren. Sie oder er kann gegenüber dem MDR keine Geldbußen verhängen.

(2) Stellt die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte Verstöße gegen Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet sie oder er dies gegenüber der Intendantin oder dem Intendanten und fordert sie oder ihn zur Stellungnahme innerhalb einer angemessenen Frist auf. Gleichzeitig unterrichtet sie oder 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 von der Intendantin oder von dem Intendanten nach Absatz 2 Satz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der Rundfunkdatenschutzbeauftragten oder des Rundfunkdatenschutzbeauftragten getroffen worden sind. Die Intendantin oder der Intendant leitet dem Verwaltungsrat gleichzeitig eine Abschrift der Stellungnahme gegenüber der Rundfunkdatenschutzbeauftragten oder dem Rundfunkdatenschutzbeauftragten zu.

(4) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte erstattet jährlich auch den Organen des MDR den schriftlichen Bericht im Sinne des Artikels 59 der Verordnung (EU) 2016/679 über ihre oder seine

Tätigkeit. Der Bericht wird veröffentlicht, wobei eine Veröffentlichung im Online-Angebot des MDR ausreichend ist.

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

(6) Die Rundfunkdatenschutzbeauftragte oder der Rundfunkdatenschutzbeauftragte ist sowohl während als auch nach Beendigung ihrer oder seiner Tätigkeit verpflichtet, über die ihr oder ihm während ihrer oder 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 Amtes 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 Rundfunkanstalt 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 Meldebehör-

den, Handelsregister, Gewerberegister und Grundbuchämter. Nichtöffentliche 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, insbesondere 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 Bei-

tragspflicht 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 Auskunftersuchen 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-Rundfunkbeitragsatzung (§§ 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
Deutsche Welle	Thomas Gardemann Ulf Bürger
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	Ivka Jurčević
Rundfunk Berlin Brandenburg	Anke Naujock-Simon
Saarländischer Rundfunk	Marion Klein
SRG SSR	Nicolina Knecht Ingo Mayer
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	Rundfunkdatenschutzbeauftragte/r
Bayerischer Rundfunk, Deutschlandradio, Saarländischer Rundfunk, Zweites Deutsches Fernsehen, Westdeutscher Rundfunk	Dr. Reinhart Binder
Deutsche Welle	Thomas Gardemann
Hessischer Rundfunk	Ulrich Göhler Simone Schlee (Stellvertreterin)
Mitteldeutscher Rundfunk	Stephan Schwarze
Norddeutscher Rundfunk	Dr. Heiko Neuhoff
Radio Bremen	Ivka Jurčević
Rundfunk Berlin Brandenburg	Anke Naujock-Simon
Südwestrundfunk	Prof. Dr. Armin Herb

12.8. Positionspapiere der Rundfunkdatenschutzkonferenz



Entschießung der RDSK zu „Clubhouse“

Clubhouse ist eine neue App für Audio-Talkshows. Über sie kann sich der App-Nutzer Gespräche anhören und an Diskussionen teilnehmen. Es sind öffentliche Diskussionen (vergleichbar virtuell gestalteten Podiumsdiskussionen), aber auch geschlossene Gruppen möglich. Ein Moderator spricht live über ein bestimmtes Thema und der Nutzer kann als Zuhörer teilnehmen. Er ist zunächst stumm geschaltet, kann aber vom Moderator zum Gespräch freigeschaltet werden. Clubhouse ist also eine Art „Live-Talkshow“ ohne Kamera (und Textnachrichten).

Datenschutzrechtlich ist diese neue App aus mehreren Gründen sehr bedenklich:

- **Zugriff auf Kontakte**

Die App erfordert den Zugriff auf alle auf dem Gerät des Nutzers gespeicherten Kontakte, wenn dieser selbst zu einer Gesprächsrunde einladen will. Er muss also die Kontaktdaten Dritter (die neben den Telefonnummern auch E-Mail-Adressen und Wohnadressen sein können) auf dem Smartphone mit Clubhouse teilen. Damit erhält Clubhouse zum einen Informationen über das soziale Umfeld des Nutzers. Zum anderen werden die Kontaktdaten von Personen, die noch nicht bei Clubhouse registriert sind, ohne deren Einwilligung an das Unternehmen übermittelt. Bei der Anmeldung über einen Social-Media-Account behält sich Clubhouse den Zugang für Follower und Freundeslisten vor.

- **Audiomitschnitte und Speicherung in den USA**

Clubhouse fertigt Audiomitschnitte, die nach eigenen Angaben ausschließlich zur Unterstützung der Untersuchung von Vorfällen aufgezeichnet werden. Diese werden ebenso wie die erhobenen Kontakt- und Accountinformationen der Nutzer und Dritter zumindest

für gewisse Zeit in den USA gespeichert und verarbeitet sowie an verschiedene Unternehmen weitergegeben. Zusagen über ein der DSGVO vergleichbares angemessenes Niveau zum Schutz dieser Daten enthält die Datenschutzerklärung des Anbieters bislang nicht. Ohne entsprechende Vorkehrungen verstößt die Datenübermittlung in die USA gegen die DSGVO (vgl. das EuGH-Urteil vom 16.7.2020, C-311/18 zum Privacy Shield).

- **Fehlende Transparenz**

In den Allgemeinen Geschäftsbedingungen („Terms of Service“) und der unzulässigerweise nur in englischer Sprache formulierten Datenschutzerklärung („Privacy Policy“) von Clubhouse wird die DSGVO bislang nicht erwähnt und eine Adresse für Datenschutzauskünfte in der EU bzw. ein Vertreter nach Art. 17 DSGVO nicht benannt. Ein Tracking kann wohl nicht verhindert werden und eine Profilbildung des Nutzers ist möglich. Wer zu den Empfängern der personenbezogenen Daten gehört und ob und in welchem Umfang Daten an Geschäftspartner verkauft werden, ist unklar und wird nicht transparent kommuniziert.

Zusammenfassend lässt sich feststellen: Von der Nutzung dieser App ist bis auf weiteres dringend abzuraten. Die RDSK fordert die Rundfunkanstalten und ihre Beteiligungsunternehmen auf, die Installation der App auf allen dienstlich zur Verfügung gestellten Geräten, mindestens aber einen Zugriff der App auf das dienstliche Kontaktverzeichnis wirksam und vollständig zu unterbinden, bis der Anbieter eine DSGVO-konforme Nutzung ermöglicht hat.

Februar 2021

Datenschutzrechtliche Eckpunkte zum Einsatz von Kollaborationssystemen

Stand: Februar 2021

I. Ausgangslage

Spätestens seit dem Inkrafttreten der coronabedingten Abstandsregelungen ist der Einsatz elektronischer Plattformen, die die ortsunabhängige Kommunikation und Zusammenarbeit zwischen mehreren Beteiligten ermöglichen (im Folgenden: Kollaborationssysteme) in den Fokus gerückt. Sie ermöglichen u. a. die folgenden Funktionen: Mailversand, Telefon- und Videokonferenz, Teamräume, Chats sowie gemeinsame Bearbeitung von Dokumenten. Besonders hoch ist die Nachfrage nach Videokonferenzen für Besprechungen, virtuelle Versammlungen, Bewerbungsgespräche, Publikumsbefragungen und vieles mehr. Angesichts der erheblichen Vorteile der virtuellen Kommunikation und Zusammenarbeit ist damit zu rechnen, dass die Kollaborationssysteme dauerhaft wichtige Werkzeuge für die Zusammenarbeit im öffentlich-rechtlichen Rundfunk und mit Externen bleiben werden.

Der Einsatz derartiger Plattformen muss allerdings datenschutzkonform sein. Denn bei ihrer Nutzung werden insbesondere folgende personenbezogene Daten verarbeitet:

- Namen und Kontaktdaten der User*innen
- Inhalte der Videokonferenz, also Ton und (Bewegt-)Bild, des Chats, der Dateien (Dokumente); dazu können auch besonders sensible Daten im Sinne von Art. 9 DSGVO gehören (z. B. körperliche Eigenschaften, politische Einstellungen etc.).
- Metadaten (z.B. zum konkreten Standort oder verwendeten Rechner)

II. Anforderungen in datenschutzrechtlicher Hinsicht

1. Schutzbedarfsfeststellung

Vor einer Auswahlentscheidung für ein Kollaborationssystem muss der Verantwortliche (im Folgenden: die Rundfunkanstalt) das angemessene Schutzniveau für die personenbezogenen Daten festlegen, die mittels der Plattform – voraussichtlich – verarbeitet werden. Die an das System zu stellenden Anforderungen in datenschutzrechtlicher Hinsicht richten sich nach dem Schutzbedarf der Daten, den die Rundfunkanstalt auf dieser Grundlage festgestellt hat. Ausschlaggebend ist die am höchsten ermittelte Schutzklasse der einzelnen Datenkategorien. Gegebenenfalls muss die Rundfunkanstalt durch geeignete technische und/oder organisatorische Maßnahmen verhindern, dass eine Kollaborationsplattform für Zwecke bzw. Anlässe genutzt wird, bei denen nicht hinreichend gewährleistet ist, dass personenbezogene Daten verarbeitet werden, die einer höheren Schutzklasse als der zugelassenen unterliegen (siehe auch III.).

2. Datenschutzrechtliche Anforderungen

Die Kollaborationsplattform muss alle zwingenden datenschutzrechtlichen Anforderungen, insbesondere die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO, u. a. Transparenz, Zweckbindung und Datensparsamkeit) sowie für die Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO) erfüllen. Die Möglichkeit datenschutzfreundlicher Voreinstellungen (Art. 25 DSGVO) muss gegeben sein. Unter den in Art. 35 DSGVO genannten Voraussetzungen muss die Rundfunkanstalt dazu gegebenenfalls eine Datenschutzfolgenabschätzung durchführen. Eine solche ist jedenfalls erforderlich, wenn das betreffende System den Einsatz neuer Technologien wie Sprach-, Gesichts- oder Stimmerkennung oder die Transkription ermöglicht bzw. vorsieht.

3. Betriebsmodelle

Grundsätzlich kann die Rundfunkanstalt wählen, ob sie eine Kollaborationsplattform selbst oder gemeinsam mit anderen Rundfunkanstalten oder Einrichtungen betreibt, oder aber den Online-Dienst eines externen Anbieters nutzt. Sofern sie sich für einen externen Dienstleister entscheidet, muss sie allerdings Folgendes beachten:

Je nachdem, um welches Fremdsystem es sich handelt, werden bei dessen Nutzung personenbezogene Daten ganz oder teilweise auf Server in Nicht-EU-Staaten, insbesondere in die USA übermittelt. Der EuGH hat mit Urteil vom 16. Juli 2020 („Schrems II“) die Privacy Shield-

Vereinbarung für unwirksam erklärt und hält zudem auch die von der EU-Kommission bislang entwickelten Standardvertragsklauseln ohne zusätzliche Garantien und Maßnahmen für keine hinreichende Rechtsgrundlage für den Datentransfer in die USA. Empfehlungen zu dahingehenden technischen und vertraglichen Maßnahmen hat der Europäische Datenschutzausschuss (EDSA) am 10. November 2020 veröffentlicht (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf).

Daraus folgt, dass Systeme von US-Anbietern wie Microsoft, Zoom oder anderen nur dann DSGVO-konform genutzt werden können, wenn die Rundfunkanstalt neben der Vereinbarung der Standardvertragsklauseln zusätzliche Garantien und Maßnahmen durchsetzt, die ein der DSGVO entsprechen des Datenschutzniveau gewährleisten.

Eine Einschränkung gilt für die Verarbeitung von streng vertraulichen personenbezogenen Daten:

Soll eine Kollaborationsplattform (auch) eingesetzt werden können, um streng vertrauliche personenbezogene Daten der Rundfunkanstalt (z. B. sensible Gesundheitsdaten oder Recherchematerial aus dem investigativen Bereich) zu verarbeiten, so ist die Wahlmöglichkeit bezüglich der Betriebsmodelle eingeschränkt. Streng vertrauliche personenbezogene Daten müssen vollständig vor dem Zugriff Externer – einschließlich dem des externen Dienstleisters – geschützt sein, z. B. durch Ende-zu-Ende-Verschlüsselung. Dies gilt insbesondere für externe Dienstleister, die ihren Sitz außerhalb der EU haben und die Anforderungen der DSGVO nicht vollständig erfüllen können. Kann ein Zugriff des externen Dienstleisters nicht vollständig ausgeschlossen werden, so muss die Rundfunkanstalt ggf. im Verbund mit den anderen Rundfunkanstalten für diese streng vertraulichen personenbezogenen Daten ein eigenes System betreiben.

4. Auftragsverarbeitung

Entscheidet sich die Rundfunkanstalt für eine durch einen externen Dienstleister betriebene Kollaborationsplattform, so wird der Anbieter in datenschutzrechtlicher Hinsicht als Auftragsverarbeiter für sie tätig. Grundlage dafür ist ein Auftragsverarbeitungsvertrag, der die Anforderungen des Art. 28 DSGVO, insbesondere Abs. 3 lit. a) - g) DSGVO erfüllen muss. Abhängig vom Ergebnis der Schutzbedarfsfeststellung muss die Rundfunkanstalt angemessene technische und organisatorische Maßnahmen (TOM) zur Gewährleistung der Informationssicherheit vereinbaren bzw. ergreifen. Dazu gehören namentlich folgende Anforderungen an die Nutzung der Kollaborationsplattform:

- Ausschalten des Aktivitätstrackings von Teilnehmer*innen
- Möglichkeit für manuelle Datenschutzeinstellungen der Nutzer*innen entsprechend der internen Vorgaben der Rundfunkanstalt
- Transportverschlüsselung nach dem Stand der Technik
- Möglichkeit der Deaktivierung von Mitschnitten einer Videokonferenz und die Möglichkeit der Vorabinformation an die Teilnehmer*innen über die Aufzeichnung
- Automatische bzw. entsprechend den Aufbewahrungsbestimmungen festgelegte Löschung eventueller Aufzeichnungen bzw. Mitschnitte nach einer Videokonferenz
- Deaktivierung der Möglichkeit zur Erstellung von Nutzungsprofilen
- Möglichkeit einer Hintergrundweichezeichnung oder eines virtuellen Hintergrundes
- Nutzerbezogener Zugang mit sicherem Authentisierungsverfahren nach dem Stand der Technik; bei Zugriff außerhalb der Rundfunkanstalt Multi-Faktor-Authentifizierung

Sofern der Anbieter seinen Sitz in einem Nicht-EU-Staat hat bzw. die Daten in einem Nicht-EU-Staat verarbeitet, muss die Rundfunkanstalt überdies prüfen, ob die Datenübermittlung in das Drittland im Einklang mit den Art. 44 ff. DSGVO steht (Näheres dazu siehe Ziffer 3).

Außerdem muss die Rundfunkanstalt ausschließen, dass der Auftragsverarbeiter die beim Betrieb seiner Plattform verarbeiteten personenbezogenen Daten ohne ordnungsgemäße Einwilligung der jeweils Beteiligten bzw. ohne gesetzliche Grundlage für eigene Zweck nutzt.

III. Organisatorische Maßnahmen zur Einhaltung von Datenschutz und Informationssicherheit

In einem internen Regelwerk (Dienstanweisung, Betriebs- oder Dienstvereinbarung) sollte die Rundfunkanstalt die einzuhaltenden technischen und organisatorischen Maßnahmen (TOM) zur Gewährleistung von Datenschutz und Datensicherheit für die Administrator*innen und alle Anwender*innen verpflichtend festhalten. Zu den dort zu regelnden Punkten sollten insbesondere gehören:

- Überblick über die datenschutzrechtlichen Risiken bei der Nutzung von Kollaborationsplattformen (Information und Sensibilisierung)

- Freigabeverfahren, das festlegt, welche Kollaborationsplattformen für die Verarbeitung welcher Datenklassen freigegeben sind bzw. welche Voraussetzungen an die Freigabe gestellt sind
- datenschutzfreundliche Voreinstellungen (z. B. Kamera und Mikrofon deaktiviert) als vorgegebener Standard
- Vorgaben zum Funktionsumfang und zu Zugriffsberechtigungen, darunter etwa die Verpflichtung zur Prüfung, ob anstatt einer Video- eine Telefonkonferenz ausreicht, Einschränkungen bzw. Modalitäten zur Nutzung der Aufzeichnungsfunktion (Mittschnitt, Screenshot, Fotografie)
- Möglichkeit, den Zugang zu Konferenzen zu schützen (z. B. Registrierung, Passwort)
- Möglichkeit der Vorfilterung externer Teilnehmer*innen (z. B. virtueller Wartebereich für Gäste bzw. Externe)
- Geeignete und verlässliche Information aller Konferenzteilnehmer*innen über die Identität der Teilnehmer*innen
- Gewährleistung, dass alle personenbezogenen Daten nach Ablauf festgelegter Löschfristen effektiv gelöscht werden
- Ausschluss einer Auswertung der Daten zur Verhaltens- oder Leistungskontrolle.

IV. Dokumentation und Information

Die für den Einsatz der jeweiligen Kollaborationsplattform verantwortliche Rundfunkanstalt muss die Anwendung gemäß Art. 30 DSGVO in ihrem Verarbeitungsverzeichnis dokumentieren (Art. 5 Abs. 2 DSGVO) und außerdem ihre zur Nutzung des Systems berechtigten oder verpflichteten Beschäftigten über die mit dem Einsatz eines solchen Systems verbundenen datenschutzrelevanten Aspekte umfassend und verständlich informieren. In den Fällen, in denen die Datenverarbeitung via Kollaborationsplattform auf die Einwilligung der Beteiligten (etwa aus anderen Rundfunkanstalten oder sonstigen Organisationen) gestützt werden soll (Art. 6 Abs. 1 lit. a) DSGVO), muss die Rundfunkanstalt die Voraussetzungen zur Einholung einer rechtswirksamen Einwilligung schaffen. Im Falle einer Verletzung des Schutzes personenbezogener Daten beim Einsatz eines solchen Systems unterliegt die jeweils verantwortliche Rundfunkanstalt der Meldepflicht nach Art. 33 DSGVO.

12.9. **Verwaltungsvereinbarungen zur Wahrung der Datenschutzaufsicht über Gemeinschaftsunternehmen und –einrichtungen der Rundfunkanstalten**

Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten vom 29. Juli 2020

Die Rundfunkdatenschutzbeauftragten

des Bayerischen Rundfunks, des Saarländischen Rundfunks, des Westdeutschen Rundfunks, des Deutschlandradio und des Zweiten Deutschen Fernsehen

des Mitteldeutschen Rundfunks des Norddeutschen Rundfunks des Südwestrundfunks
sowie

der Beauftragte für den Datenschutz der Deutschen Welle

(im Folgenden: Aufsichtsbehörden) schließen zur Wahrnehmung der Datenschutzaufsicht über die Unternehmen, an denen die von ihnen zu beaufsichtigenden Rundfunkanstalten insgesamt oder teilweise unmittelbar oder mittelbar gemeinschaftlich beteiligt sind (Gemeinschaftsunternehmen), folgende Vereinbarung:

§ 1 Federführung

(1) Die Aufsicht über jedes Gemeinschaftsunternehmen nimmt eine Aufsichtsbehörde federführend wahr. Ihre Handlungen und Erklärungen wirken im Verhältnis zum Gemeinschaftsunternehmen für und gegen die anderen Aufsichtsbehörden.

(2) Die Federführungen und die jeweils beteiligten Aufsichtsbehörden ergeben sich aus der als Anlage 1 beigefügten Übersicht.

(3) Die Aufgaben und Befugnisse jeder beteiligten Aufsichtsbehörde nach den Art. 57 f. DSGVO bzw. den jeweils maßgeblichen gesetzlichen Vorschriften bleiben von einer Federführung unberührt.

§ 2 Zuständigkeit der federführenden Aufsichtsbehörde

(1) Die federführende Aufsichtsbehörde ist zuständig für die Entgegennahme und Bearbeitung von Meldungen nach Art. 33 DSGVO. Die federführende Aufsichtsbehörde nimmt im Verhältnis zum jeweiligen Gemeinschaftsunternehmen die Aufgaben und Befugnisse wahr, die sich aus der DSGVO bzw. den jeweils maßgeblichen gesetzlichen Vorschriften ergeben.

(2) Die federführende Aufsichtsbehörde ist primärer Ansprechpartner für die oder den jeweilige/n Datenschutzbeauftragte/n des Gemeinschaftsunternehmens nach Art. 37 DSGVO.

§ 3 Abstimmung zwischen dem Federführer und den anderen Aufsichtsbehörden

(4) Soweit nachfolgend nicht anderweitig geregelt, nimmt der jeweilige Federführer die Aufgaben der Aufsicht eigenständig wahr. Die anderen beteiligten Aufsichtsbehörden sind berechtigt, vom Federführer jederzeit Auskunft über etwaige Empfehlungen, aufsichtsrechtliche Verfahren oder Maßnahmen zu verlangen oder ihn zu solchen Verfahren oder Maßnahmen aufzufordern.

(5) Der Federführer informiert die anderen beteiligten Aufsichtsbehörden vorab über eine Empfehlung bzw. Maßnahme im Rahmen einer vorherigen Konsultation nach Art. 36 DSGVO, eine Datenschutzüberprüfung nach Art. 58 Abs. 1 lit. b) DSGVO oder die Verhängung einer Geldbuße nach Art. 58 Abs. 2 lit. i) DSGVO und gibt ihnen Gelegenheit zur Stellungnahme innerhalb einer Frist von mindestens drei Wochen. Beabsichtigt der Federführer, sich einem innerhalb dieser Frist eingegangenen Änderungswunsch anzuschließen, legt er den beteiligten Aufsichtsbehörden einen überarbeiteten Entwurf vor und gibt ihnen Gelegenheit zur erneuten Stellungnahme innerhalb von 12 Werktagen. Sofern innerhalb dieser Frist ein weiterer Widerspruch eingeht, wiederholt er das Verfahren nach Satz 1 und 2. An eine auf dieser Grundlage vorgenommene aufsichtsrechtliche Handlung des Federführers sind die beteiligten Aufsichtsbehörden gebunden.

(6) Das Recht jeder beteiligten Aufsichtsbehörde, sich an einer vom Federführer beabsichtigten Datenschutzüberprüfung nach Art. 58 Abs. 2 lit. i) DSGVO zu beteiligen, bleibt hiervon unberührt.

(7) Der Federführer stellt jeder beteiligten Aufsichtsbehörde auf Wunsch alle relevanten Informationen und Daten zur Aufsicht über das betreffende Gemeinschaftsunternehmen für ihren jeweiligen Tätigkeitsbericht oder sonstige Anlässe zur Verfügung.

§ 4 Informationsaustausch

Der Federführer und die anderen beteiligten Aufsichtsbehörden tauschen untereinander alle zweckdienlichen Informationen zur Aufsicht über das jeweilige Beteiligungsunternehmen aus.

§ 5 Geltungsdauer, Kündigung

(1) Die Vereinbarung tritt am 1. Januar 2020 in Kraft und gilt zunächst bis zum 31. Dezember 2022. Sie verlängert sich um jeweils ein weiteres Jahr, sofern nicht eine der Vertragsparteien spätestens zum 30. September eines Kalenderjahres kündigt.

(2) Die Kündigung kann schriftlich oder per mail erklärt und muss allen Vertragspartnern zugestellt werden. Für die Wirksamkeit der Kündigung genügt der fristgemäße Eingang bei einem der Vertragspartner.

§ 6 Sonstiges

(1) Mündliche Nebenabreden sind unwirksam. Jede Änderung dieser Vereinbarung einschließlich dieser Vorschrift bedarf der Schriftform und des Einvernehmens aller Vertragsparteien.

(2) Änderungen der Anlage 1 lassen die Geltung der Verwaltungsvereinbarung unberührt. Im Übrigen gilt Absatz 1 entsprechend.

Anlage 1:

Gemeinschaftsunternehmen, beteiligte Aufsichtsbehörden, Federführung

**Anlage zur
Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten**
Stand: September 2020

Gemeinschaftsunternehmen, Sitz	Gesellschafter	Zuständige RDSB	Federführung
ARD-Werbung SALES & SERVICES GmbH, Frankfurt/M	BRmedia GmbH 11,11 %	BR, MDR, NDR, SR, SWR, WDR	RDSB SR
	hr werbung GmbH 11,11 %		
	MDR-Werbung GmbH 11,11 %		
	NDR Media GmbH 11,11 %		
	Radio Bremen Media GmbH 11,11 %		
	rbb media GmbH 11,11 %		
	Werbefunk Saar GmbH 11,11 %		
	SWR Media Services GmbH 11,11 %		
WDR mediagroup GmbH 11,11 %			
ARD.ZDF medienakademie gGmbH, Nürnberg	BR HR 12,90 6,05 %	BR, MDR, NDR, SR, SWR, WDR, DW, DRadio, ZDF	RDSB BR
	MDR 8,55 %		
	NDR 14,00		
	RB 0,65%		
	RBB 5,30 %		
	SR 1,00 %		
	SWR 14,60%		
	WDR 16,80%		
	DR 2,50 %		
	DW 5,65 %		
ZDF 12,00%			

ARTE Deutschland GmbH, Baden-Baden	BR 7,26 % HR 3,50 % MDR 5,26 % NDR 8,12 % RB 1,24 % RBB 4,00 % SR 1,24 % SWR 8,38 % WDR 11,00 ZDF 50,00	BR, MDR, NDR, SR, SWR, WDR, ZDF	RDSBSWR
AS&S Radio GmbH, Frankfurt/M	ARD-Werbung Sales & Services GmbH 100 %	BR, MDR, NDR, SR, SWR, WDR	RDSB SR
Baden-Badener Pensionskasse WaG, Baden-Baden	Bayerischer Rundfunk Deutsche Welle Deutsch- landradio Hessischer Rundfunk Mitteldeutscher Rundfunk Norddeutscher Rundfunk Radio Bremen Rundfunk Berlin-Brandenburg Saarländischer Rundfunk Süd- westrundfunk Westdeutscher Rundfunk ARTE Deutschland TV GmbH ARD.ZDF medienakademie gGmbH BRmedia GmbH Degeto Film GmbH Deutsche Fernsehlotterie gGmbH	BR, MDR, NDR, SR, SWR, WDR, DRadio	RDSB SWR

	Stiftung Deutsches Rundfunkarchiv hr Media Lizenz- und Verlags GmbH hr werbung GmbH Institut für Rundfunktechnik GmbH NDR Media GmbH ProFunk GmbH rbb media GmbH SWR Media Services GmbH WDR mediagroup GmbH WDR mediagroup dialog GmbH WDR mediagroup digital GmbH		
Bavaria Film GmbH, München	WDR Mediagroup GmbH 33,35 % Bavaria Filmkunst GmbH 16,67 % SWR media services GmbH 16,67 % LfA Gesellschaft für Vermögensverwaltung GmbH 16,67 % Drefa Medien Holding 16,64 %	BR, MDR, SWR, WDR	RDSB BR
DEGETO Film GmbH, Frankfurt/M	BR 11,11 % hr werbung GmbH 11,11 % MDR 11,11 % NDR Media GmbH 11,11 % RB 11,11 % RBB 11,11 % Werbefunk Saar GmbH 11,11 % SWR 11,11 % WDR mediagroup GmbH 11,11 %	BR, MDR, NDR, SR, SWR, WDR	RDSB NDR
Deutsches Rundfunkarchiv (DRA), Frankfurt/M	BR 7,14 % HR 7,14 %	BR, MDR, NDR, SR, SWR, WDR, DRadio, DW	RDSB DRadio

	MDR 7,14 % NDR 7,14 % RB 7,14 % RBB 14,28% SR 7,14 % SWR 14,28 WDR 7,14 % DR 14,28 DW 7,14 %		
Innovations- und Digitalagentur (ida) GmbH	MDR 51 % ZDF Digital Medienproduktion 49 %	MDR, ZDF	ROSS MDR
Institut für Rundfunktechnik GmbH (IRT), München	BR 9,29% HR 5,71 % MDR 5,71 % NDR 9,29 % RB 5,71 % RBB 5,71 % SR 5,71 % SWR 11,43% WDR 9,29 % DR 5,71 % DW 5,71 % ORF 5,71 % SRG 5,71 % ZDF 9,29%	BR, MDR, NDR, SR, SWR, WDR, DRadio, ZDF	ROSS BR
Pensionskasse Rundfunk WaG, Frankfurt/M	BR DW	BR, MDR, NDR, SR, SWR, WDR	ROSS WDR

	DRadio HR MDR NDR RB RBB SR SWR WDR Degeto Film GmbH Weitere Beteiligungsgesellschaften und Produktionsunternehmen		
Saxonia Media Filmproduktionsgesellschaft mbH, Leipzig	Bavaria Film 51 % Drefa Media Holding 49 %	BR, MDR	RDSB MDR
SportA GmbH, München	BR 5,56 % HR 5,56 % MDR 5,56 % NDR 5,56 % RB 5,56 % RBB 5,56 % SR 5,56 % SWR 5,56 % WDR 5,56 % ZDF 50,00 %	BR, MDR, NDR, SR, SWR, WDR, ZDF	RDSB BR

Verwaltungsvereinbarung
zur Wahrnehmung der Datenschutzaufsicht
über Gemeinschaftseinrichtungen der Rundfunkanstalten

vom 29. Juli 2020

Die Mitglieder der RDSK (im Folgenden: Aufsichtsbehörden) schließen zur Wahrnehmung der Datenschutzaufsicht über die rechtlich unselbstständigen Gemeinschaftseinrichtungen der Rundfunkanstalten folgende Vereinbarung:

§ 1 Federführung

(1) Die Aufsicht über jede Gemeinschaftseinrichtung nimmt ein Mitglied der RDSK federführend wahr. Ihre bzw. seine Handlungen und Erklärungen wirken im Verhältnis zu den für die Gemeinschaftseinrichtung Verantwortlichen für und gegen die anderen Aufsichtsbehörden.

(2) Die Federführungen ergeben sich aus der als Anlage 1 beigefügten Übersicht.

(3) Die Aufgaben und Befugnisse jeder beteiligten Aufsichtsbehörde nach den Art. 57 f. DSGVO bzw. den jeweils maßgeblichen gesetzlichen Vorschriften bleiben von einer Federführung unberührt.

§ 2 Zuständigkeit der federführenden Aufsichtsbehörde

(1) Die federführende Aufsichtsbehörde ist zuständig für die Entgegennahme und Bearbeitung von Meldungen nach Art. 33 DSGVO.

(2) Die federführende Aufsichtsbehörde nimmt im Verhältnis zu den für die jeweilige Gemeinschaftseinrichtung Verantwortlichen die Aufgaben und Befugnisse wahr, die sich für die Datenschutzaufsicht aus der DSGVO bzw. den jeweils maßgeblichen gesetzlichen Vorschriften ergeben.

(3) Die federführende Aufsichtsbehörde ist primärer Ansprechpartner für die oder den jeweilige/n Datenschutzbeauftragte/n der Gemeinschaftseinrichtung nach Art. 37 DSGVO.

§ 3 Abstimmung zwischen dem Federführer und den anderen Aufsichtsbehörden

(1) Soweit nachfolgend nicht anderweitig geregelt, nimmt der jeweilige Federführer die Aufgaben der Aufsicht eigenständig wahr. Die anderen beteiligten Aufsichtsbehörden sind berechtigt, vom Federführer jederzeit Auskunft über etwaige aufsichtsrechtliche Empfehlungen, Verfahren oder Maßnahmen zu verlangen oder ihn zu solchen Verfahren oder Maßnahmen aufzufordern.

(2) Der Federführer informiert die anderen beteiligten Aufsichtsbehörden vorab über eine Empfehlung oder Maßnahme im Rahmen einer vorherigen Konsultation nach Art. 36

DSGVO oder eine Datenschutzüberprüfung nach Art. 58 Abs. 1 lit. b) DSGVO und gibt ihnen Gelegenheit zur Stellungnahme innerhalb einer Frist von mindestens zwölf Werktagen. Beabsichtigt der Federführer, sich einem innerhalb dieser Frist eingegangenen Änderungswunsch anzuschließen, legt er den beteiligten Aufsichtsbehörden einen überarbeiteten Entwurf vor und gibt ihnen Gelegenheit zur erneuten Stellungnahme innerhalb von zwölf Werktagen. Sofern innerhalb dieser Frist ein weiterer Widerspruch eingeht, wiederholt er das Verfahren nach Satz 1 und 2. An eine auf dieser Grundlage vorgenommene aufsichtsrechtliche Handlung des Federführers sind die beteiligten Aufsichtsbehörden gebunden.

(3) Das Recht jeder beteiligten Aufsichtsbehörde, sich an einer vom Federführer beabsichtigten Datenschutzüberprüfung nach Art. 58 Abs. 2 lit. i) DSGVO zu beteiligen, bleibt hiervon unberührt.

(4) Der Federführer stellt jeder beteiligten Aufsichtsbehörde auf Wunsch alle relevanten Informationen und Daten zur Aufsicht über die betreffende Gemeinschaftseinrichtung für ihren jeweiligen Tätigkeitsbericht oder sonstige Anlässe zur Verfügung.

§ 4 Informationsaustausch

Der Federführer und die anderen beteiligten Aufsichtsbehörden tauschen untereinander alle zweckdienlichen Informationen zur Aufsicht über die jeweilige Gemeinschaftseinrichtung aus.

§ 5 Geltungsdauer, Kündigung

(1) Die Vereinbarung tritt am 1. Januar 2020 in Kraft und gilt zunächst bis zum 31. Dezember 2022. Sie verlängert sich um jeweils ein weiteres Jahr, sofern nicht eine der Vertragsparteien spätestens zum 30. September eines Kalenderjahres kündigt.

(2) Die Kündigung kann schriftlich oder per mail erklärt und muss allen Vertragspartnern zugestellt werden. Für die Wirksamkeit der Kündigung genügt der fristgemäße Eingang bei einem der Vertragspartner.

§ 6 Sonstiges

(1) Mündliche Nebenabreden sind unwirksam. Jede Änderung dieser Vereinbarung einschließlich dieser Vorschrift bedarf der Schriftform und des Einvernehmens aller Vertragsparteien.

(2) Änderungen der Anlage 1 lassen die Geltung der Verwaltungsvereinbarung unberührt. Im Übrigen gilt Absatz 1 entsprechend.

Anlage 1: Gemeinschaftseinrichtungen, beteiligte Anstalten, Federführung

Anlage zur
Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht
über Gemeinschaftseinrichtungen der Rundfunkanstalten
Stand: September 2020

GSEA	Beteiligte Rundfunkanstalten (Federführung)	Federführendes RDSK-Mitglied
ARD aktuell	Alle Landesrundfunkanstalten (NDR)	RDSB NDR
Ard.de	Alle Landesrundfunkanstalten (SWR)	RDSB SWR
ARD Generalsekretariat	Alle Landesrundfunkanstalten (rbb/gf. Anstalt)	DSB rbb
ARD HSB	Alle Landesrundfunkanstalten (rbb/WDR)	DSB rbb
ARD Play-Out-Center	Alle Landesrundfunkanstalten (rbb)	DSB rbb
ARD Sternpunkt	Alle Landesrundfunkanstalten (HR)	DSB HR
ARD./DRadio Steuerbüro	Alle Landesrundfunkanstalten + DRadio (MDR)	RDSB MDR
ARD Text	Alle Landesrundfunkanstalten (rbb)	DSB rbb
Beitragsservice Von ARD, ZDF und Deutschlandradio	Alle Landesrundfunkanstalten, DRadio, ZDF (WDR)	Beitragszahler/innen: Jew. RDSB von BR, MDR, NDR, SR, SWR, WDR. Im Übrigen: RDSB WDR
Boerse.de	Alle Landesrundfunkanstalten (HR)	DSB HR
3sat	ZDF, alle Landesrundfunkanstalten (ZDF)	RDSB ZDF
EU-Verbindungsbüro in Brüssel	Alle Landesrundfunkanstalten (WDR)	RDSB WDR
funk	Alle Landesrundfunkanstalten, ZDF (SWR)	RDSB SWR
Geschäftsstelle der ARD-Gremienkonferenz	Alle Landesrundfunkanstalten (BR)	RDSB BR
IVZ	Mitglieder ARD, DRadio (rbb)	DSB rbb
KEF Büro der ARD	Alle Landesrundfunkanstalten (NDR)	RDSB NDR
KiKA	Alle Landesrundfunkanstalten, ZDF (MDR)	RDSB MDR
One	Alle Landesrundfunkanstalten (WDR)	RDSB WDR
Phoenix	Alle Landesrundfunkanstalten, ZDF (ZDF/WDR)	RDSB ZDF

Programmdirektion DFS/ daserste.de	Alle Landesrundfunkanstalten (BR)	RDSB BR
Sportschau.de	Alle Landesrundfunkanstalten (WDR)	RDSB WDR
Tagesschau24 / tageschau.de	Alle Landesrundfunkanstalten (NDR)	RDSB NDR

12.10. Jahresbericht 2021 des bDSB für den Kinderkanal von ARD/ZDF

Jahresbericht 2021

Betrieblicher Datenschutz im KiKA

1. bDSB – Weiterbildungen, Tagungen und Veranstaltungen	
21.06	MDR, Social Media Veranstaltung mit TikTok & Facebook

2. Audits im KiKA	
	Coronabedingt ausgefallen - jährliches Datenschutzgespräch im KiKA

3. Arbeitskreise und -gemeinschaften	
21.01	AK MDR-Datenschutzkoordinatoren, #4 Sitzung
21.04	AK DSB, Webkonferenz #1/2
21.06	AK DSB Sondersitzung
21.07	AK MDR-Datenschutzkoordinatoren, Sondersitzung
21.11	AK DSB, Webkonferenz #2/2

4. Organisatorische Maßnahmen	
21.08	Anpassung Datenschutzerklärungen – Web & App
21.10	Dial Systems (eSponse) – Spam-awareness
21.11	KiKA Quiz App – Projektunterstützung – App-Launch

5. Abgeschlossene red.spezifische Aufgaben und Problemstellungen	
21.01	Presselounge – Backend-Lücke
21.01	Presselounge - Nutzerdaten
21.01	Mitmachaktion - Mit der Maus
21.01	Nutzung von Sprachassistenten im KiKA
21.02	Ghostery-Nielsen – AGF - Datenschutzerklärung
21.02	Gewinnspiel Jodel-Challenge
21.02	AppCenter - Absturzberichte - App DSE
21.03	Weitergabe von Emailadressen-Freienrat
21.03	Kommentare-Webpage-Schloss Einstein
21.03	Casting-Junior ESC
21.03	Mitmachaktion – Schloss Einstein - Jubiläum-Aktion
21.03	Nutzung des Verbreitungsweges: TikTok
21.03	Gewinnspiel – Ene Meine Bu
21.04	ARD Nutzeranmeldung-Apps
21.04	Mitmachaktion – Junior ESC - Teilnahmeaufruf
21.04	Mitmachaktion – KiKA-Award - Teilnahmeaufruf
21.04	TeamTimster - Zuschauerbefragung
21.05	Telefonmitschnitte Kummerkasten
21.05	Produzentenveranstaltung
21.05	Telemedien-Änderungskonzept (TMÄK) der ARD
21.05	ARD-Login für Minderjährige
21.05	UrhG_Datamining

21.05	Ablösung DVDs im Materialzentrum
21.05	Voting Pinpoll und GoogleReCaptcha
21.05	MDR TikTok_Testballon-Schloss Einstein
21.06	25 Jahre KiKA – Mitmachaktion über WhatsApp-Kanal
21.06	Internes EM-Tippspiel
21.06	Cookiebanner & Zählpixel
21.06	Mitmachaktion – DBKD- Zuschaueraktion
21.06	EVK –Ene mene Bu
21.06	Datenschutzerklärung und gendergerechte Sprache
21.07	Mitmachaktion – Abenteuer Sommeraktion
21.07	Weitergabe Store-Accounts
21.08	Rich Harvest Medienforschung
21.08	Datenschutzerklärung – Roku-Streaming-Plattform
21.08	Mitmachaktion – Schloss Einstein - Zurück zur Schule
21.08	Mitmachaktion – Schloss Einstein - Meet&Greet
21.08	Mitmachaktion – Zoes-Zauberschrank - Bilder-Uploadaktion
21.08	Bewerbungsformular DbKD
21.08	Alexa Sprachsteuerung
21.09	Nutzung „virtuelle Fotobox“
21.09	Mitmachaktion – #SayHi
21.09	Mitmachaktion – Schloss Einstein Hexenwochenende
21.10	Mitmachaktion-Weihnachten-Gedichte
21.10	Personalisierung Mediathek
21.10	Castingaufruf: Run4You
21.12	Cookie-Popup bei Gewinnspielen
21.12	Kinderredaktionsrat

6. Externe Unterstützungsanfragen		
21.05	LVZ (Postdienstleister) Cyberangriff	LVZ
21.08	Personalisierung der Mediatheken	ZDF
21.08	EVK – Dreh mit Kindern	MDR

7. Laufende senderspezifische Problemstellungen	
21.08	Alexa Sprachsteuerung
21.12	Cookie-Popup bei Gewinnspielen
21.12	Kinderredaktionsrat

8. Auskunftersuche	
21.03	Auskunft-Löschung

9. Strafverfolgungen	
21.04	Kommentar auf Elternseiten
21.11	Youtubekanal – Bummi - Kikaninchen.de – Fremdbetrieb

10. spezielle Mitarbeitersensibilisierung	
	Die Mitarbeitersensibilisierung findet im Zusammenhang mit Ersteinweisungen statt.