18. Tätigkeitsbericht

der Beauftragten für den Datenschutz

des

Rundfunk Berlin-Brandenburg

Berichtszeitraum:

1. April 2021 bis 31. März 2022

dem Rundfunkrat gemäß § 38 Abs. 7 rbb-Staatsvertrag

vorgelegt von

Anke Naujock-Simon

Inhaltsverzeichnis

Abkürzungsverzeichnis

AK DSB	Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio
ARD-GS	ARD-Generalsekretariat
BAG	Bunderarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BlnDSG	Berliner Datenschutzgesetz
BMJ	Bundesministerium der Justiz
BND-Gesetz	Bundesnachrichtendienst-Gesetz
BPersVG	Bundespersonalvertretungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BR	Bayerischer Rundfunk
BVerfG	Bundesverfassungsgericht
CAFM	Computer-Aided Facility Management
CC ISec	Corporation Center Information Security (Zusammenschluss der Informationssicherheitsbeauftragten von ARD, ZDF und Deutschlandradio)
CISPE CoC	CoC (Verhaltenskodex) für Cloud Service Provider
CoC	Codes of Conduct
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
DA	Dienstanweisung
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung

DSK	Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
EDSA	Europäischer Datenschutz-Ausschuss
EG	Erwägungsgrund
ems	electronic media school
EGMR	Europäischer Gerichtshof für Menschenrechte
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FSZ	Fernsehzentrum (rbb)
GG	Grundgesetz
GeschGehG	Geschäftsgeheimnisgesetz
GRCh	Charta der Grundrechte der Europäischen Union
GSEA	Gemeinschaftseinrichtung der ARD
GO	Geschäftsordnung
HA	Hauptabteilung
HA GM	Hauptabteilung Gebäudemanagement
HA MIT	Hauptabteilung Mediensysteme und IT
HdR	Haus des Rundfunks (rbb)
HmbBfDI	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit
HR	Hessischer Rundfunk
HSB	ARD-Hauptstadtstudio
i. d. F.	in der Fassung
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IVZ	Informationsverarbeitungszentrum
JuKo	Juristische Kommission
KEF	Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten
KI	Künstliche Intelligenz

LG	Landgericht
MÄStV	Medienänderungsstaatsvertrag
MDR	Mitteldeutscher Rundfunk
MIT	Mediensysteme und IT
MStV	Medienstaatsvertrag
NDR	Norddeutscher Rundfunk
NetzDG	Netzwerkdurchsetzungsgesetz
NetzDGÄndG	Netzwerkdurchsetzungsgesetz-Änderungsgesetz
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
POC	Proof of Concept
PAN	Presse-Archiv-Netzwerk
OTT-Dienste	Over-The-Top-Dienste
RÄndStV	Rundfunkänderungsstaatsvertrag
RB	Radio Bremen
rbb	Rundfunk Berlin-Brandenburg
rbb-StV	Staatsvertrag über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg (rbb-Staatsvertrag)
RBStV	Rundfunkbeitragsstaatsvertrag
RDSK	Rundfunkdatenschutzkonferenz
RStV	Rundfunkstaatsvertrag
SolMan	Solution Manager
SR	Saarländischer Rundfunk
SWR	Südwestrundfunk
TKG	Telekommunikationsgesetz
TKMoG	Telekommunikationsmodernisierungsgesetz 2021
TMG	Telemediengesetz
TOM	technische und organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz

UC	Unified Communication
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
VG	Verwaltungsgericht
VV	Verwaltungsvereinbarung
VVT	Verzeichnis von Verarbeitungstätigkeiten
WDR	Westdeutscher Rundfunk
ZBS	Zentraler Beitragsservice

Vorbemerkung

Mit diesem Tätigkeitsbericht wird die Entwicklung des Datenschutzes beim Rundfunk Berlin-Brandenburg (rbb) für den Zeitraum vom 1.4.2021 bis 31.3.2022 dokumentiert. Der Tätigkeitsbericht umfasst meine Aktivitäten als Beauftragte für den Datenschutz im journalistisch-redaktionellen Bereich und als betriebliche Datenschutzbeauftragte im wirtschaftlich-administrativen Bereich.

Im zurückliegenden Jahr hat die Corona-Pandemie erneut meine Arbeitsbedingungen bestimmt und zahlreiche datenschutzrechtliche Fragen im Zusammenhang mit der Umsetzung der sich immer wieder ändernden Abstandsregelungen aufgeworfen. Wie in den vergangenen Jahren, so bedurfte auch im Berichtsjahr der Einsatz und die Einführung weiterer Anwendungen der Bürokommunikationssoftware Microsoft 365 im rbb einer intensiven Begleitung durch die Datenschutzbeauftragte. Auf ARD-Ebene hat insbesondere die Koordination der Erarbeitung der neuen Leitlinien zum Datenschutz in den Telemedien-Angeboten von ARD, ZDF und Deutschlandradio das Berichtsjahr maßgeblich für mich geprägt. Die wachsende Bedeutung der Telemedien-Angebote, die Entwicklung immer neuer Formate und die Erschließung immer neuer Verbreitungswege erfordern es, dass die Rundfunkdatenschutzbeauftragten den damit zusammenhängenden datenschutzrechtlichen Fragen einen hohen Stellenwert einräumen.

Die Digitalisierung schreitet in allen Bereichen des rbb weiter voran. Zeitgleich steigt die Bedrohungslage. Der rbb ist daher – wie alle anderen Rundfunkanstalten – gezwungen, den Schutz seiner IT-Systeme massiv zu erhöhen. IT-Sicherheit dient zwar immer auch dem Datenschutz; die Maßnahmen zur IT-Sicherheit können andererseits aber auch den Datenschutz für die von den Maßnahmen Betroffenen einschränken. Hier gilt es, einen angemessenen Ausgleich zu finden. Darauf werde ich bei der datenschutzrechtlichen Begleitung auch weiterhin achten.

Meiner Assistentin Frau Ulrike Stephan und meinem Assistenten Herrn Michel Brzozowski danke ich für ihr Engagement und ihre tatkräftige Unterstützung. Herrn Axel Kauffmann danke ich für seine gewissenhafte Vertretung. Bei den Datenschutz-Koordinator:innen bedanke ich

mich für ihren Einsatz dafür, die Themen Datenschutz und Datensicherheit in den Direktionen bzw. Gemeinschaftseinrichtungen stärker zu verankern. Den Kollegen aus der Informationssicherheit danke ich für die konstruktive Zusammenarbeit. Schließlich danke ich der Intendantin und allen weiteren Mitgliedern der Geschäftsleitung wieder für ihr Vertrauen und ihre Unterstützung.

Dieser Tätigkeitsbericht umfasst eine Auswahl der wichtigsten Themen des zurückliegenden Jahres. Aus Zeitgründen konnten nicht sämtliche Aktivitäten der Datenschutzbeauftragten Erwähnung finden. Der Bericht wird – wie alle Vorgängerberichte – im Online-Angebot des rbb veröffentlicht, abrufbar unter:

http://www.rbb-online.de/unternehmen/der_rbb/struktur/datenschutz/datenschutz_im_rbb.html

A. Die Stellung der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg

I. Gesetzliche Grundlagen

Gemäß § 38 Abs. 1 rbb-Staatsvertrag (rbb-StV) bestellt der Rundfunkrat einen Beauftragten oder eine Beauftragte für den Datenschutz. Er bzw. sie ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen und untersteht im Übrigen der Dienstaufsicht des rbb-Verwaltungsrates. Gemäß Abs. 2 Satz 1 überwacht er bzw. sie die Einhaltung der Datenschutzvorschriften des rbb-StV und anderer Vorschriften über den Datenschutz, soweit der rbb personenbezogene Daten zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet.

Soweit eine Befugnis des oder der Beauftragten für den Datenschutz nach Abs. 2 Satz 1 nicht gegeben ist, obliegt die Kontrolle der Einhaltung von Datenschutzbestimmungen beim rbb dem oder der Landesbeauftragten für den Datenschutz des Landes Berlin. Die Kontrolle erfolgt im Benehmen mit dem oder der Landesbeauftragten des Landes Brandenburg (Abs. 8).

Für die Sicherstellung des Datenschutzes im wirtschaftlich-administrativen Bereich ist beim rbb – wie bei allen Berliner Behörden und sonstigen öffentlich-rechtlichen Stellen – außerdem ein:e betriebliche:r Datenschutzbeauftragte:r sowie jeweils ein:e Stellvertreter:in zu bestellen. Diese Pflicht ergibt sich aus § 36 Abs. 1 rbb-StV i. V. m. § 4 Abs. 1 des Berliner Datenschutzgesetzes (BlnDSG).

Die Aufgaben und Befugnisse der Aufsicht werden durch Art. 51 ff. Datenschutz-Grundverordnung (DSGVO) konkretisiert. Gemäß Art. 57 DSGVO haben die datenschutzrechtlichen Aufsichtsbehörden – und damit auch die rbb-Datenschutzbeauftragte im journalistisch-redaktionellen Bereich – u. a. folgende Aufgaben:

- Überwachung und Durchsetzung der Einhaltung der DSGVO,

- Beratung, Aufklärung und Sensibilisierung der Verantwortlichen und der Öffentlichkeit für die Risiken im Zusammenhang mit der Verarbeitung von personenbezogenen Daten,
- Bearbeitung von Datenschutzbeschwerden,
- Zusammenarbeit mit den anderen datenschutzrechtlichen Aufsichtsbehörden und
- Erstellung eines jährlichen Tätigkeitsberichts.

Nach Art. 39 DSGVO hat der bzw. die betriebliche Datenschutzbeauftragte – und damit auch die rbb-Datenschutzbeauftragte im wirtschaftlich-administrativen Bereich – mindestens folgende Aufgaben zu erfüllen:

- Unterrichtung und Beratung der Verantwortlichen und der Beschäftigten, die Datenverarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie sonstiger Datenschutzvorschriften,
- kontinuierliche Überwachung der Einhaltung der datenschutzrechtlichen Bestimmungen sowie der Strategien der Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und diesbezügliche Überprüfungen,
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung (DSFA) und Überwachung ihrer Durchführung und
- Zusammenarbeit mit der Aufsichtsbehörde als Ansprechpartner:in in Fragen der Verarbeitung personenbezogener Daten, einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO und gegebenenfalls Beratung zu allen sonstigen Fragen.

Die Gegenüberstellung der Aufgaben der Aufsichtsbehörde und der betrieblichen Datenschutzbeauftragten zeigt viele Überschneidungen. In der Praxis macht es für die Datenschutzbeauftragte des rbb kaum einen Unterschied, ob sie in der einen oder anderen Funktion tätig wird, zumal sie auch im wirtschaftlich-administrativen Bereich oftmals erste Anlaufstelle für datenschutzrechtliche Fragen und Beschwerden ist.

Die Aufgaben der rbb-Datenschutzbeauftragten sind detailliert in der Dienstanweisung Informationsmanagement (s. Tz. 4.1 der Anlage 2 ‚Datenschutz') beschrieben.

II. Konkrete Situation

Auf seiner Sitzung vom 20.6.2019 hat mich der Rundfunkrat gemäß § 38 Abs. 1 rbb-StV auf Vorschlag der Intendantin für eine weitere Amtszeit von vier Jahren für den Zeitraum vom 1.7.2019 bis 30.6.2023 zur Beauftragten für den Datenschutz bestellt. Parallel dazu hat mich die Intendantin für den gleichen Zeitraum zur betrieblichen Datenschutzbeauftragten gemäß § 4 Abs. 1 BlnDSG ernannt. Ich nehme die Funktion der Rundfunkdatenschutzbeauftragten gemäß § 38 Abs. 1 rbb-StV und der betrieblichen Datenschutzbeauftragten gemäß § 4 BlnDSG hauptamtlich und in Personalunion wahr. Zusätzlich bekleide ich seit 1.7.2019 das Amt der Compliance-Beauftragten.

Seit dem 1.4.2014 ist der Leiter der internen Revision, Herr Axel Kauffmann, stellvertretender betrieblicher Datenschutzbeauftragter. Herr Kauffmann vertritt mich in Abwesenheitsfällen.

Im Sommer 2021 hat meine Assistentin Frau Ulrike Stephan ihre Arbeitszeit auf 50% reduziert. Im Umfang der verbliebenen 50% hat seit Juli 2021 Herr Michel Brzozowski Assistenz-Aufgaben für die Datenschutzbeauftragte übernommen.

Seit Juli 2020 bildet die rbb-Datenschutzbeauftragte Rechtsreferendar:innen aus.

B. Entwicklung des Datenschutzrechts

I. Europa

1. Verordnungen und Richtlinien

1.1 Datenschutz-Grundverordnung

Seit dem 25.5.2018 ist die Datenschutz-Grundverordnung (DSGVO) in allen Mitgliedsstaaten der Europäischen Union direkt geltendes Recht.

Für Auslegungsfragen sind vor allem die Leitlinien, Empfehlungen und Orientierungshilfen des Europäischen Datenschutzausschusses (EDSA) und die Rechtsprechung des Europäischen Gerichtshofs (EuGH) maßgeblich.

Der EDSA besteht aus der Leitung einer Aufsichtsbehörde jedes Mitgliedsstaates und dem bzw. der Europäischen Datenschutzbeauftragten (Art. 68 Abs. 3 DSGVO). Ist in einem Mitgliedsstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe der DSGVO erlassenen Vorschriften zuständig, so wird im Einklang mit den Rechtsvorschriften dieses Mitgliedsstaates ein Gemeinsamer Vertreter benannt (Art. 68 Abs. 4 DSGVO). § 17 Abs. 1 Bundesdatenschutzgesetz (BDSG) legt fest, dass die Funktion des Gemeinsamen Vertreters der deutschen Aufsichtsbehörden im EDSA von dem bzw. der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) wahrgenommen wird. Zum Stellvertreter des Gemeinsamen Vertreters hat der Bundesrat am 25.6.2021 den Bayerischen Landesbeauftragten für den Datenschutz, Herrn Prof. Dr. Thomas Petri, gewählt. Zuvor hatten die Aufsichtsbehörden der Länder den Hamburgischen Datenschutzbeauftragten mit der Wahrnehmung ihrer Interessen im EDSA betraut, nachdem der Bundesrat zunächst keine:n Stellvertreter:in gewählt hatte.

1.2 Entwurf E-Privacy-Verordnung

Die E-Privacy-Verordnung soll Vorgaben zum Datenschutz bei der Bereitstellung und Nutzung von Telemediendiensten, klassischen Kommunikationsdiensten wie Telefonie und SMS und

internetbasierten Kommunikationsdiensten, insbesondere Messengern wie Skype oder WhatsApp, regeln. Ursprünglich sollte sie zeitgleich mit der DSGVO in Kraft treten. Über den Stand des Verordnungsentwurfs habe ich in der Vergangenheit wiederholt berichtet (zuletzt im 17. Tätigkeitsbericht, S. 5). Im Februar 2021 hat sich der EU-Ministerrat unter dem Vorsitz von Portugal auf einen neuen Entwurf geeinigt. Dieser bleibt aus Datenschutzsicht hinter den bisherigen Entwürfen zurück. Er sieht vor, dass Metadaten von Nutzenden verarbeitet werden dürfen, wenn es dafür „kompatible“ Gründe gibt. Außerdem sind darin weitreichende Ausnahmen vom Einwilligungserfordernis beim Setzen von Cookies enthalten. Derzeit finden die sogenannten Trilog-Verhandlungen statt. Der Trilog ist ein paritätisch zusammengesetztes Dreiertreffen der gesetzgebenden Institutionen EU-Kommission, EU-Ministerrat und EU-Parlament. Mit der Verabschiedung der E-Privacy-Verordnung ist realistisch nicht vor 2024 zu rechnen.

1.3 Entwurf der Verordnung zur Regulierung Künstlicher Intelligenz

Am 21.4.2021 hat die EU-Kommission ihren Verordnungsentwurf zur Regulierung von Künstlicher Intelligenz (KI) in Europa vorgestellt. Hintergrund ist der rasche Fortschritt der KI. Während diese Schlüsseltechnologie weitgehende Vorteile wirtschaftlicher und gesellschaftlicher Art verspricht, gehen mit ihrer Nutzung auch erhöhte Risiken einher. Ziel ist es daher gemäß der Begründung des Entwurfs, Europa einerseits zu einer führenden Kraft im Bereich der KI zu entwickeln und andererseits einen rechtlichen Rahmen zu setzen, der die Werte, Prinzipien und Rechte der Europäischen Union schützen kann. In dem Entwurf werden die KI-Systeme anhand der damit verbundenen Risiken klassifiziert und bestimmte Praktiken verboten. Außerdem enthält der Entwurf weitgehende Transparenzpflichten. Der Verordnungsentwurf muss nun zunächst das übliche Gesetzgebungsverfahren auf EU-Ebene durchlaufen.

Für die Zukunft sind auch im öffentlich-rechtlichen Rundfunk Einsatzfelder für KI denkbar. Im Rahmen von Projekten wird diese Technologie schon heute im Bereich der Produktion und Archivierung von Video- und Audiomaterial beim rbb eingesetzt (s. Kap. C. V. 2.). Insofern muss das weitere Gesetzgebungsverfahren aufmerksam beobachtet werden.

2. Angemessenheitsbeschlüsse der EU-Kommission

2.1. Großbritannien

Zum 31.1.2020 ist Großbritannien aus der EU ausgetreten. Nach dem Auslaufen entsprechender Übergangsregelungen hat die EU-Kommission am 28.6.2021 zwei Angemessenheitsbeschlüsse zum Vereinigten Königreich angenommen – einen im Rahmen der DSGVO und einen im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung. Beide Beschlüsse sind an diesem Tag in Kraft getreten. Personenbezogene Daten können nun auch weiterhin ungehindert aus der EU in das Vereinigte Königreich fließen, denn dort gilt laut EU-Kommission ein Schutzniveau, das dem nach dem EU-Recht garantierten Schutzniveau vergleichbar ist.

Ausschlaggebend für diese Einschätzung der EU-Kommission waren folgende Aspekte:

- Das Datenschutzsystem des Vereinigten Königreichs basiert weiterhin auf denselben Regeln, die galten, als das Vereinigte Königreich noch Mitgliedsstaat der EU war.
- In Bezug auf den Zugriff auf personenbezogene Daten durch Behörden im Vereinigten Königreich (insbesondere aus Gründen der nationalen Sicherheit) sieht das System des Vereinigten Königreichs starke Garantien vor. Die Datenerhebungen durch Nachrichtendienste unterliegen der vorherigen Genehmigung durch ein unabhängiges Rechtsorgan.

Die Angemessenheitsbeschlüsse der EU-Kommission enthalten eine Verfallklausel, die ihre Geltungsdauer begrenzt: Beide Beschlüsse laufen vier Jahre nach ihrem Inkrafttreten aus. Sie können danach erneuert werden, falls das Vereinigte Königreich weiterhin ein angemessenes Datenschutzniveau sicherstellt.

Die Rundfunkanstalten arbeiten insbesondere im technischen Bereich auch mit Dienstleistern aus Großbritannien zusammen. Insofern ist es sehr erfreulich, dass es für den Datentransfer der Rundfunkanstalten nach Großbritannien mit dem Angemessenheitsbeschluss weiterhin eine sichere Rechtsgrundlage gibt.

2.2 USA

Wie berichtet, hat der EuGH mit Urteil vom 16.7.2020 die Regelungen des EU-US Privacy Shield für ungültig erklärt (s. 17. Tätigkeitsbericht, S. 7 f.). Auf seiner Basis dürfen daher keine Datenübermittlungen mehr in den Gültigkeitsbereich US-amerikanischen Rechts vorgenommen werden. Damit ist eine wichtige Rechtsgrundlage für den Datentransfer in die USA weggefallen. Aktuell kann der rbb nur noch mit US-amerikanischen Dienstleistern zusammenarbeiten, wenn die sogenannten Standardvertragsklauseln vereinbart werden und zusätzlich durch geeignete technische und organisatorische Maßnahmen (TOM) erreicht werden kann, dass die Daten im Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. In der Praxis sind diese Anforderungen nur sehr schwer umzusetzen. Die Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 25.1.2022 ein Gutachten des Rechtsexperten Prof. Steven Vladeck mit Antworten auf Fragen zum aktuellen Stand des US-Überwachungsrechts veröffentlicht. Prof. Vladeck war schon im Schrems-II-Verfahren vor dem irischen Gericht als Gutachter aufgetreten. Das Gutachten kommt zu dem Ergebnis, dass die Rechtslage nach wie vor komplex ist und Schwierigkeiten für europäische Bürgerinnen und Bürger bestehen, Rechtsschutz gegen unrechtmäßige Eingriffe der US-Ermittlungsbehörden zu erlangen.

Im März 2022 haben sich die EU und die USA grundsätzlich auf ein neues Abkommen geeinigt. Künftig sollen Regeln und Garantien den Zugriff der US-Geheimdienste auf die Daten beschränken, die zur Verfolgung definierter nationaler Sicherheitsziele notwendig und verhältnismäßig sind. Zudem soll es unabhängigen Rechtsschutz für die Beschwerden von Europäer:innen geben. Ein konkreter Rechtstext liegt noch nicht vor. Erst wenn dies der Fall ist, kann der Prozess auf EU-Ebene für einen sogenannten Angemessenheitsbeschluss beginnen. Dabei müssen der EDSA sowie die EU-Staaten und das Europäische Parlament einbezogen werden.

3. Neue Standardvertragsklauseln

Mit dem Schrems II-Urteil vom 16.7.2020 hat der EuGH die Anforderungen an die Verwendung von Standardvertragsklauseln als Rechtsgrundlage für den Datentransfer in Drittstaaten in der Praxis ganz erheblich verschärft (s. dazu 17. Tätigkeitsbericht, S. 8 f.). Danach liegt es in der

Verantwortung eines Datenexporteurs, vor der Übermittlung personenbezogener Daten zu prüfen, ob in dem Drittland ein Schutzniveau für personenbezogene Daten besteht, das dem in der EU gleichwertig ist. Dabei geht es vor allem um die Frage, ob der Datenexporteur beim Abschluss von Standardvertragsklauseln und unter Berücksichtigung zusätzlicher Maßnahmen Grund zu der Annahme haben muss, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur im Drittland geltenden Rechtsvorschriften und Gepflogenheiten diesen an der Erfüllung seiner Pflichten aus den Standardvertragsklauseln hindern. Die EU-Kommission hat im Juni 2021 unter Berücksichtigung der erhöhten Anforderungen neue Standardvertragsklauseln erlassen. Diese sind modular aufgebaut und können in folgenden Transfer-Konstellationen eingesetzt werden:

1. Verantwortlicher an Verantwortlichen (Modul 1)
2. Verantwortlicher an Auftragsverarbeiter (Modul 2)
3. Auftragsverarbeiter an (Unter-)Auftragsverarbeiter (Modul 3)
4. Rückübermittlung des Auftragsverarbeiters in der EU an einen Verantwortlichen im Drittland (Modul 4)

Für den rbb ist insbesondere Modul 2 relevant, da er in unterschiedlichen Konstellationen mit US-amerikanischen Dienstleistern im Rahmen von Auftragsverarbeitungsverhältnissen zusammenarbeitet.

In den neuen Standardvertragsklauseln verpflichtet sich der Datenimporteur, Betroffene bei Anfragen von Ermittlungsbehörden zu benachrichtigen und zur Vermeidung der Erteilung der von einer Ermittlungsbehörde verlangten Auskunft im äußersten Fall alle verfügbaren Rechtsmittel auszuschöpfen. Die neuen Standardvertragsklauseln sind seit dem 27.9.2021 zwingend für Neuverträge zu verwenden. Spätestens bis zum 27.12.2022 muss eine Umstellung sämtlicher Altverträge auf die neuen Standardvertragsklauseln erfolgt sein.

4. Empfehlungen des EDSA zu Datentransfers in Drittländer

Anknüpfend an die vom EuGH im sogenannten Schrems II-Urteil festgestellte Notwendigkeit, für die Übermittlung von personenbezogenen Daten in die USA zusätzlich zu den Standardvertragsklauseln ergänzende Schutzmaßnahmen zu treffen, hatte der EDSA am 10.11.2020

entsprechende Empfehlungen vorgelegt (s. dazu 17. Tätigkeitsbericht, S. 10). Sie zielen darauf ab, den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern Hinweise zu geben, wie sie feststellen können, ob zusätzlich zum Abschluss der Standardvertragsklauseln ergänzende Maßnahmen erforderlich sind, um ein im Wesentlichen gleichwertiges Schutzniveau für die in Drittländer übermittelten Daten zu gewährleisten. Außerdem beziehen sich die Empfehlungen auf die konkret zu ergreifenden Maßnahmen. Im Juni 2021 hat der EDSA nach öffentlicher Konsultation die endgültige Fassung der Empfehlungen zu ergänzenden Maßnahmen angenommen. Diese enthält einige Änderungen bzw. Klarstellungen. So betont der EDSA die Bedeutung der Prüfung der Praktiken von Behörden aus Drittländern bei der rechtlichen Bewertung durch dieDatenexporteure, um festzustellen, ob die Rechtsvorschriften und/oder die Praktiken des Drittlands in der Praxis die Wirksamkeit der Standardvertragsklauseln beeinträchtigen. Stellt sich bei der Prüfung heraus, dass die bloße Vereinbarung der Klauseln zur Wahrung eines angemessenen Datenschutzniveaus nicht ausreichend ist, was insbesondere bei überbordenden Zugriffsbefugnissen von ausländischen Sicherheitsbehörden der Fall sein kann, müssen zusätzliche Garantien geschaffen werden. Als technische Maßnahmen empfiehlt der EDSA – wie schon in der ersten Fassung – insbesondere Verschlüsselungstechniken und die Pseudonymisierung von Daten.

Der EDSA bekräftigt noch einmal seine Auffassung, dass Ausnahmen für bestimmte Fälle von Drittlandübermittlungen (Art. 49 DSGVO) eng auszulegen sind.

5. Abschluss Kohärenzverfahren CoC EU Cloud und CISPE

Erstmalig hat der EDSA im Rahmen eines Kohärenzverfahrens in zwei Fällen bestätigt, dass Verhaltensregeln, sogenannte Codes of Conduct (CoC), den Anforderungen der DSGVO entsprechen. Die Einhaltung eines genehmigten CoC soll Vertrauen und Transparenz schaffen und den Risiko-Bewertungsprozess für Kunden erleichtern. Der EU Cloud CoC konkretisiert die Anforderungen des Art. 28 DSGVO zur Auftragsverarbeitung und der damit verbundenen Vorschriften der DSGVO für Cloud-Anbieter. Die DSGVO schreibt eine unabhängige Überwachungsstelle vor, um die angemessene Umsetzung der genehmigten Verhaltensregeln zu gewährleisten. Im Mai 2021 wurde SCOPE Europe von der belgischen Datenschutzbehörde offiziell als dedizierte Überwachungsstelle des EU Cloud CoC akkreditiert.

Der CISPE CoC ist wie der EU Cloud CoC ein europäischer Verhaltenskodex für Cloud Service Provider. Er bezieht sich auf Provider, die Cloud-Infrastruktur-Services anbieten (CISPE = Cloud Infrastructure Services Providers in Europe). Bei der Auswahl der Cloud-Service-Provider sollte der rbb zukünftig darauf achten, dass sich die Anbieter dem CoC bzw. CISPE CoC unterworfen haben.

6. Beschluss des EDSA in einem Dringlichkeitsverfahren gegenüber Facebook

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat am 11.5.2021 eine Anordnung erlassen, die es der Facebook Ireland Ltd. verbot, personenbezogene Daten von WhatsApp zu verarbeiten, soweit dies zu eigenen Zwecken erfolgte. Der sofortige Vollzug wurde angeordnet. Der HmbBfDI begründete diese Maßnahme mit einer befürchteten datenschutzwidrigen Weitergabe personenbezogener Daten durch WhatsApp (Unternehmen von Facebook, jetzt Meta) an Facebook Ireland Ltd. Mit seinen zum 15.5.2021 geänderten Nutzungsbedingungen lässt sich WhatsApp u. a. die Möglichkeit der Datenweitergabe an Drittunternehmen – ausdrücklich auch an Facebook – einräumen (ohne die Zustimmung kann die App nicht mehr genutzt werden). Die irische Datenschutzbehörde hatte als federführende Behörde trotz Aufforderung durch den HmbBfDI eine aufsichtsbehördliche Überprüfung der Verarbeitungsvorgänge zwischen WhatsApp und Facebook nicht vorgenommen. Seinem Wortlaut nach sieht Art. 66 Abs. 1 DSGVO vor, dass eine Aufsichtsbehörde „unter außergewöhnlichen Umständen“ einstweilige Maßnahmen erlassen kann, wenn nach ihrer Auffassung „dringender Handlungsbedarf besteht“, um die Rechte und Freiheiten Betroffener zu schützen. Erlaubt sind der betroffenen Aufsichtsbehörde nur auf drei Monate befristete Maßnahmen und auch nur mit Wirkung auf das betroffene Hoheitsgebiet. Nachdem der HmbBfDI einen verbindlichen Beschluss der EDSA beantragt hatte, hat dieser am 15.7.2021 entschieden, dass die Voraussetzungen für den Nachweis des Vorliegens eines Verstoßes und einer Dringlichkeit nicht erfüllt sind. Angesichts der verschiedenen Widersprüche, Unklarheiten und Unsicherheiten, die in den Nutzerinformationen von WhatsApp und in schriftlichen Erklärungen von Facebook und WhatsApp festgestellt wurden, kam der EDSA zu dem Schluss, dass er nicht in der Lage sei, mit Sicherheit festzustellen, welche Verarbeitungen tatsächlich durchgeführt werden und auf welche Art und Weise. Der EDSA hat die irische Aufsichtsbehörde daher aufgefordert, vorrangig eine Untersuchung durchzuführen, um festzustellen, ob

solche Verarbeitungstätigkeiten stattfinden oder nicht, und wenn dies der Fall ist, ob sie eine ordnungsgemäße Rechtsgrundlage gemäß Art. 5 Abs. 1 lit. a) und Art. 6 Abs. 1 DSGVO haben. Nach Vorlage eines Beschlussentwurfs der irischen Aufsichtsbehörde erließ der EDSA am 28.7.2021 einen sogenannten Streitbeilegungsbeschluss auf der Grundlage von Art. 65 DSGVO. Was die Transparenz betrifft, so führt der Beschlussentwurf der irischen Aufsichtsbehörde bereits einen schwerwiegenden Verstoß gegen die Art. 12, 13 und 14 DSGVO an. Der EDSA hat in den bereitgestellten Informationen jedoch noch zusätzliche Mängel festgestellt. Der Beschlussentwurf der irischen Aufsichtsbehörde enthielt die Anweisung, die Verarbeitungstätigkeiten innerhalb von 6 Monaten in Einklang mit der DSGVO zu bringen. Der EDSA hielt es für äußerst wichtig, die Transparenzverpflichtungen so schnell wie möglich zu erfüllen. Vor diesem Hintergrund wurde die irische Aufsichtsbehörde ersucht, die sechsmonatige Frist für die Einhaltung auf drei Monate zu verkürzen.

7. Leitlinien des EDSA zum Auskunftsrecht Betroffener

Der EDSA hat am 18.1.2022 die Leitlinien 01/2022 zu den Rechten der betroffenen Person – Recht auf Auskunft – angenommen und diese zur öffentlichen Konsultation freigegeben. Die Leitlinien sollen anhand von Beispielen und Erläuterungen in Zukunft den für die Verarbeitung Verantwortlichen dabei helfen, Auskunftsersuchen in einer der DSGVO entsprechenden Weise zu beantworten. Eine deutsche Fassung der Leitlinien liegt noch nicht vor.

II. Bund

1. Gesetze

1.1 Telekommunikation-Telemedien-Datenschutz-Gesetz

Am 1.12.2021 ist das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten. Dieses Gesetz enthält spezifische Datenschutzvorschriften für Anbieter von Telekommunikationsdiensten (z. B. Telefonprovider) und Telemediendiensten (Websites oder Apps). Die bisher nicht an die DSGVO angepassten Datenschutzvorschriften des Telekommunikationsgesetzes (TKG) und Telemediengesetzes (TMG) wurden überarbeitet, ausgegliedert

und in dem neuen TTDSG zusammengefasst. Umgesetzt wurden ferner die Vorgaben der E-Privacy-Richtlinie. Die Vorschriften des TTDSG stehen neben denen der DSGVO. Notwendig ist daher nun immer eine zweigleisige Prüfung. Wichtig für die Rundfunkanstalten ist insbesondere § 25 TTDSG, der für den Einsatz von Cookies und sogenannter Local-Storage-Elemente einen Einwilligungsvorbehalt vorsieht. Während es in der DSGVO um den Schutz personenbezogener Daten geht, schützt § 25 TTDSG die Integrität des Endgeräts. Grundsätzlich ist für das Setzen von Cookies und Local-Storage-Elementen eine Einwilligung erforderlich (§ 25 Abs. 1 TTDSG). Gemäß § 25 Abs. 2 TTDSG bedarf es ausnahmsweise keiner Einwilligung, wenn deren Einsatz „unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom jeweiligen Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann“ (§ 25 Abs. 2 Ziffer 2). Nach Auffassung der Rundfunkdatenschutzbeauftragten greift diese Ausnahme bei der anonymisierten statistischen Nutzungsmessung von Online-Angeboten. Auch nach der DSGVO ist dafür keine Einwilligung erforderlich, weil das Angebot von Telemedien und die Überprüfung, ob diese überhaupt von den Nutzer:innen nachgefragt werden, zu den gesetzlichen Aufgaben der Rundfunkanstalten gehört (Art. 6 Abs. 1 Satz 1 lit. e) DSGVO).

Ich habe die zuständigen Bereiche um eine Bestandsaufnahme der im rbb verwendeten Cookies und Local-Storage-Elemente gebeten, um anschließend bei der rechtlichen Einordnung unterstützen zu können.

1.2 Telekommunikationsmodernisierungsgesetz

Am 1.12.2021 ist auch das Telekommunikationsmodernisierungsgesetz 2021 (TKMoG) in Kraft getreten. Es schreibt neben den Änderungen im Telekommunikationsgesetz auch Änderungen in knapp sechzig weiteren Gesetzen vor. Mit der umfassenden Novelle des Telekommunikationsgesetzes ist ein Ordnungsrahmen geschaffen worden, der die technische Entwicklung im Telekommunikationssektor, etwa mit Blick auf sogenannte Over-The-Top-Dienste (OTT) wie z. B. Messenger-Dienste, abbildet und Impulse für einen schnelleren und flächendeckenden Ausbau von Gigabit-Netzen geben soll. OTT-Dienste sind Inhalte, die mittels einer Internetverbindung angeboten werden, ohne dass die Internetanbieter selbst Einfluss oder Kontrolle über den Inhalt haben. Bei dem neuen Ordnungsrahmen geht es darum, gezielte Anreize für Investitionen und Innovationen zu setzen sowie den marktgetriebenen Ausbau der digitalen

Infrastruktur durch Flexibilisierung der Regulierungsvorgaben und neuen Regulierungsinstrumente voranzubringen.

1.3 Änderung des Netzwerkdurchsetzungsgesetzes

Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) ist seit dem 1.10.2017 in Kraft. Das Gesetz zielt darauf ab, Hass-Kriminalität, strafbare Falschnachrichten und andere strafbare Inhalte auf den Plattformen sozialer Netzwerke wirksamer zu bekämpfen. Dies beinhaltet eine gesetzliche Berichtspflicht für Anbieter sozialer Netzwerke über den Umgang mit Hass-Kriminalität und anderen strafbaren Inhalten, Vorgaben zum Vorhalten eines wirksamen Beschwerde-Managements sowie zur Benennung eines inländischen Zustellungsbevollmächtigten. Verstöße gegen diese Pflichten können mit Bußgeldern gegen das Unternehmen und die Aufsichtspflichtigen geahndet werden. Außerdem wird Opfern von Persönlichkeitsrechts-Verletzungen im Netz ermöglicht, aufgrund gerichtlicher Anordnung die Bestandsdaten der Verletzer:innen von den Diensteanbietern zu erhalten.

Zur Stärkung der Strafverfolgung in sozialen Netzwerken wurde das NetzDG mit dem am 3.4.2021 in Kraft getretenen Gesetz zur Bekämpfung des Rechtsextremismus und der Hass-Kriminalität um eine Meldepflicht erweitert. Anbieter sozialer Netzwerke sind nunmehr verpflichtet, besonders schwere Straftaten an eine Zentralstelle beim Bundeskriminalamt (BKA) zu melden. Die Anbieter müssen den Inhalt und die zur Verfügung stehenden Daten des Inhaltsverfassers bzw. der Inhaltsverfasserin (inkl. der letzten Log-In-IP) an das BKA übermitteln. Es soll anschließend die Täter:innen identifizieren und die Daten an die zuständigen Strafverfolgungsbehörden weiterleiten.

Mit dem am 28.6.2021 in Kraft getretenen NetzDGÄndG wurden die Rechte der Nutzer:innen sozialer Netzwerke gestärkt. Sie können in Zukunft effektiver gegen Entscheidungen der Anbieter sozialer Netzwerke vorgehen, wenn unterschiedliche Auffassungen in Bezug auf das Löschen oder Beibehalten einzelner Beiträge bestehen. Darüber hinaus können Betroffene von strafbaren Beiträgen wie Beleidigungen oder Bedrohungen ihre Auskunftsansprüche gegenüber sozialen Netzwerken in Zukunft noch leichter durchsetzen.

Bei unterschiedlichen Auffassungen zwischen Nutzer und Anbieter eines sozialen Netzwerks, ob gemeldete Inhalte gelöscht werden müssen oder nicht, kann künftig ein Gegenvorstellungsverfahren durchgeführt werden. Dadurch werden soziale Netzwerke dazu verpflichtet, auf Antrag eines Nutzers/einer Nutzerin Entscheidungen über die Löschung oder Beibehaltung eines Inhalts zu überprüfen, wobei das Ergebnis dieser Überprüfung der Person gegenüber in jedem Einzelfall zu begründen ist.

1.4 IT-Sicherheitsgesetz 2.0

Das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – kurz IT-Sicherheitsgesetz 2.0 – vom 18.5.2021 ist nach Verkündung mit drei Ausnahmen am 28.5.2021 in Kraft getreten. Seit 1.12.2021 gilt das IT-Sicherheitsgesetz 2.0 vollständig. Ihm voraus ging ein langwieriges Gesetzgebungsverfahren von rund zwei Jahren. Das Gesetz bezweckt eine Anpassung und Weiterentwicklung der Schutzmechanismen und Abwehrstrategien im Bereich der IT-Sicherheit und regelt hierzu ein Bündel von Einzelmaßnahmen. Für das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das Gesetz einen erheblichen Verantwortungs- und Aufgabenzuwachs mit sich gebracht.

Aufgrund der Staatsferne des öffentlich-rechtlichen Rundfunks und aus Gesetzgebungskompetenzgründen gilt das IT-Sicherheitsgesetz für die öffentlich-rechtlichen Rundfunkanstalten nicht. Nichtsdestotrotz orientieren sie sich an den dort definierten Anforderungen für die sogenannte kritische Infrastruktur (Näheres dazu siehe 17. Tätigkeitsbericht, S. 17 ff.).

1.5 Gesetz zur Novellierung des Bundespersonalvertretungsgesetzes

Am 15.6.2021 ist das neue Bundespersonalvertretungsgesetz (BPersVG) vom 6.6.2021 in Kraft getreten. Das BPersVG kommt über einen entsprechenden Verweis im rbb-StV zur Anwendung.

Bislang war die Frage, ob der Personalrat für die Verarbeitung von personenbezogenen Daten zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben eigenständiger Verantwortlicher oder nur Teil der verantwortlichen Dienststelle ist, in der Rechtslehre nicht eindeutig geklärt. Diese Unsicherheit ist durch den neuen § 69 beendet.

§ 69 mit dem Titel ‚Datenschutz' lautet:

„Bei der Verarbeitung personenbezogener Daten hat der Personalrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Personalrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist die Dienststelle der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Die Dienststelle und der Personalrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften."

Die Folgen aus dieser gesetzlichen Klarstellung ergeben sich aus der amtlichen Begründung zu § 69 :

„Als Akteur der Verarbeitung einer Vielzahl personenbezogener, teils sensibler, Beschäftigtendaten hat der Personalrat die datenschutzrechtlichen Vorschriften einzuhalten (Satz 1). Diese ergeben sich insbesondere aus der DSGVO und dem BDSG. Von besonderer Bedeutung ist § 26 BDSG, welcher spezifische Bestimmungen zur Verarbeitung personenbezogener Daten von Beschäftigten durch die Interessenvertretung der Beschäftigten enthält. Kern der Regelung ist die Festlegung der seit dem Inkrafttreten der DSGVO umstrittenen datenschutzrechtlichen Verantwortlichkeit für die Verarbeitung personenbezogener Daten durch den Personalrat. Satz 2 weist diese der Dienststelle zu. Dies ist sachgerecht, da der Personalrat lediglich eine organisationsinterne Einrichtung, jedoch keine nach außen rechtlich verselbständigte Institution ist. Bei der Verarbeitung personenbezogener Daten agiert der Personalrat daher als institutionell unselbständiger Teil der für die Einhaltung des Datenschutzes verantwortlichen Dienststelle. Die Regelung führt die bislang bestehende Rechtslage fort und macht von der durch Artikel 4 Nummer 7 zweiter Halbsatz der DSGVO eröffneten Möglichkeit Gebrauch, den für die Datenverarbeitung Verantwortlichen im mitgliedsstaatlichen Recht zu bestimmen. Die beiderseitige Unterstützungspflicht von Dienststelle und Personalrat bei der Einhaltung der datenschutzrechtlichen Vorschriften (Satz 3) beruht auf der datenschutzrechtlichen Verantwortlichkeit der Dienststelle einerseits und der innerorganisatorischen Selbständigkeit und Weisungsfreiheit des Personalrats andererseits. Bei der Erfüllung der datenschutzrechtlichen Pflichten sind Dienststelle und Personalrat daher in vielfacher Weise auf gegenseitige Unterstützung angewiesen: So hat der Personalrat keine Pflicht, ein eigenes Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 DSGVO) zu führen, allerdings muss das Verarbeitungsverzeichnis der

Dienststelle auch die Verarbeitungstätigkeiten des Personalrats enthalten. Auch bei den datenschutzrechtlichen Auskunftsrechten (Artikel 15 DSGVO) ist die Dienststelle, wenn der Auskunftsanspruch sich auf die durch den Personalrat verarbeiteten Daten bezieht, auf die Unterstützung durch den Personalrat angewiesen. Schließlich hat der Personalrat innerhalb seines Zuständigkeitsbereichs eigenverantwortlich die Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit im Sinne der Artikel 24 und 32 DSGVO sicherzustellen. Die Dienststelle hat den Personalrat mit den hierfür erforderlichen Sachmitteln, wie etwa geeigneten Sicherungseinrichtungen für Unterlagen mit personenbezogenen Daten, auszustatten (§ 47). Die Stellung und die Aufgaben des behördlichen Datenschutzbeauftragten richten sich nach der DSGVO (Artikel 38 und 39) und bestehen somit auch gegenüber dem Personalrat als Teil der verantwortlichen Stelle. Soweit erforderlich, sollte der Personalrat die Beratung durch den behördlichen Datenschutzbeauftragten in Anspruch nehmen."

Konkret bedeutet dies:

- ⇨ Die Verfahren im Personalrat, bei denen personenbezogene Daten verarbeitet werden, müssen beschrieben und ins rbb-Verzeichnis von Verarbeitungstätigkeiten (VVT) aufgenommen werden. (Einer entsprechenden gegenüber dem Personalrat nach Änderung des BPersVG ausgesprochenen Einladung der Datenschutzbeauftragten ist der Personalrat bislang nicht gefolgt. Die Dokumentation muss jetzt zügig nachgeholt werden.)

- ⇨ Datenschutzrechtliche Auskunftsersuchen gegenüber dem rbb beziehen sich auch auf die Datenverarbeitung durch den Personalrat. Bei der Klärung, ob personenbezogene Daten des Antragstellers/der Antragstellerin durch den rbb verarbeitet werden, ist der Personalrat mit einzubeziehen.

- ⇨ Für den Personalrat gelten die gleichen hohen Anforderungen an den Datenschutz und die Informationssicherheit, wie im gesamten rbb.

Noch eine andere Regelung des neuen BPersVG ist datenschutzrechtlich relevant. Gemäß § 38 Abs. 3 finden die Sitzungen des Personalrats in der Regel als Präsenzsitzungen in Anwesenheit seiner Mitglieder vor Ort statt:

„Die Sitzung kann vollständig oder unter Zuschaltung einzelner Personalratsmitglieder mittels Video- oder Telefonkonferenz durchgeführt werden, wenn

1. *vorhandene Einrichtungen genutzt werden, die durch die Dienststelle zur dienstlichen Nutzung freigegeben worden sind,*
2. *nicht mindestens ein Viertel der Mitglieder oder die Mehrheit der Vertreterinnen und Vertreter einer Gruppe des Personalrats binnen einer von der oder dem Vorsitzenden zu bestimmenden Frist gegenüber der oder dem Vorsitzenden widerspricht und*
3. *der Personalrat geeignete organisatorische Maßnahmen trifft, um sicherzustellen, dass Dritte vom Inhalt der Sitzung keine Kenntnis nehmen können.*

Eine Aufzeichnung ist unzulässig. Personalratsmitglieder, die mittels Video- oder Telefonkonferenz an Sitzungen teilnehmen, gelten als anwesend (…). Das Recht eines Personalratsmitglieds auf Teilnahme an der Sitzung vor Ort bleibt durch die Durchführung der Sitzung mittels Video- oder Telefonkonferenz unberührt." (§ 38 Abs. 3 Satz 2–4).

Dem gesetzlichen Verbot einer Aufzeichnung der Video- bzw. Telefonkonferenz entsprechen die internen Regelungen des rbb für die Nutzung des Videokonferenzsystems Microsoft Teams, wonach die Aufzeichnung von Besprechungen mit streng vertraulichen Inhalten ausgeschlossen ist.

1.6 Entwurf Hinweisgeberschutzgesetz

In Deutschland ist der Schutz von sogenannten Whistleblowern bislang vor allem durch die Rechtsprechung geprägt. Dabei orientieren sich die Gerichte der Zivil- und Arbeitsgerichtsbarkeit an den Vorgaben des Europäischen Gerichtshofs für Menschenrechte (EGMR). Das Bundesministerium der Justiz (BMJ) hat am 13.4.2022 einen Referentenentwurf zur Umsetzung der Richtlinie 2019/1037 (Hinweisgeberschutzrichtlinie) „zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden" veröffentlicht. Diese Richtlinie musste von den

Mitgliedsstaaten bis zum 17.12.2021 in nationales Recht umgesetz werden. Das BMJ hatte bereits im Dezember 2020 einen Referentenentwurf zur Umsetzung der Richtlinie in Deutschland in die Ressortabstimmung gegeben. Dieser habe laut BMJ allerdings wegen des Widerspruchs damals unionsgeführter Ressorts nicht veröffentlicht werden können. Das Gesetz regelt den Schutz von natürlichen Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die in dem Gesetz vorgesehenen Meldestellen weitergeben oder offenlegen („hinweisgebende Personen"). Darüber hinaus hat das Gesetz auch den Schutz derjenigen Personen im Blick, die Gegenstand einer Meldung oder Offenlegung sind, sowie sonstige Personen, die von einer Meldung oder Offenlegung betroffen sind. In dem Gesetzentwurf ist beschrieben, welche Meldestellen zu errichten sind und wie diese zu arbeiten haben. Es wird eine ausdrückliche Rechtsgrundlage zur Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Bearbeitung von Meldungen geschaffen. „Interessierte Kreise" hatten bis zum 11.5.2022 Gelegenheit, zu dem Entwurf Stellung zu nehmen.

Der weitere Fortgang des Gesetzgebungsverfahrens muss aufmerksam begleitet werden. Der rbb hat seit 2015 eine Compliance-Beauftragte bestellt. Die Compliance-Beauftragte ist Ansprechpartnerin für alle fest angestellten und freien Mitarbeiter:innen des rbb sowie aller Bürgerinnen und Bürger, die Anhaltspunkte für regelwidriges Verhalten im rbb haben. Seit 2019 hat die rbb-Datenschutzbeauftragte die Funktion der Compliance-Beauftragten inne. Aus dem Referenten-Entwurf für das Hinweisgeberschutzgesetz ergibt sich für den rbb derzeit kein Handlungsbedarf.

2. Entscheidungen

2.1 Beschluss des Bundesverfassungsgerichts zur Unterlassung der Zustimmung zum Ersten Medienänderungsstaatsvertrag durch das Land Sachsen-Anhalt

Wie berichtet, hat das Land Sachsen-Anhalt dem Ersten Medienänderungsstaatsvertrag (MÄStV) nicht zugestimmt (s. 17. Tätigkeitsbericht, S. 25 f.). Darin war eine Anhebung des monatliche Rundfunkbeitrags um 86 Cent von 17,50 EUR auf 18,36 EUR ab dem 1.1.2021 vorgesehen. Durch die Unterlassung der Zustimmung konnte der Staatsvertrag nicht zum 1.1.2021

in Kraft treten. Gegen diese Unterlassung haben ARD, ZDF und Deutschlandradio gemeinsam Verfassungsbeschwerde eingelegt. Mit dem am 5.8.2021 veröffentlichten Beschluss vom 20.7.2021 (1 BvR 2756/20; 1 BvR 2775/20; 1 BvR 2777/20) hat das Bundesverfassungsgericht (BVerfG) entschieden, dass das Land Sachsen-Anhalt durch das Unterlassen seiner Zustimmung zum Ersten MÄStV die Rundfunkfreiheit der öffentlich-rechtlichen Rundfunkanstalten aus Artikel 5 Abs. 1 Satz 2 GG verletzt hat. Die Bestimmungen des Artikels 1 des Ersten MÄStV – mit der darin vorgesehenen Anpassung des Rundfunkbeitrags – gelten vorläufig seit 20.7.2021 bis zum Inkrafttreten einer staatsvertraglichen Neuregelung über die funktionsgerechte Finanzierung von ARD, ZDF und Deutschlandradio. Von einer Anordnung der rückwirkenden Erhöhung des Rundfunkbeitrags zum 1.1.2021 hat das BVerfG abgesehen.

Zur Begründung hat es – anknüpfend an seine bisherige rundfunkverfassungsrechtliche Judikatur – bekräftigt, dass den öffentlich-rechtlichen Rundfunkanstalten ein grundrechtlicher Finanzierungsanspruch zustehe. Die Erfüllung dieses Anspruchs obliege der Ländergesamtheit als föderaler Verantwortungsgemeinschaft, wobei jedes Land Mitverantwortungsträger sei. Die Rundfunkfreiheit diene der freien, individuellen und öffentlichen Meinungsbildung. Der in Art. 5 Abs. 1 Satz 2 GG enthaltene Auftrag zur Gewährleistung der Rundfunkfreiheit ziele auf eine Ordnung, die sicherstellt, dass die Vielfalt der bestehenden Meinungen im Rundfunk in größtmöglicher Breite und Vollständigkeit Ausdruck findet. Dabei wachse die Bedeutung der dem beitragsfinanzierten öffentlich-rechtlichen Rundfunk obliegenden Aufgabe, durch authentische, sorgfältig recherchierte Informationen, die Fakten und Meinungen auseinanderhalten, die Wirklichkeit nicht verzerrt darzustellen und das Sensationelle nicht in den Vordergrund zu rücken, vielmehr ein vielfaltssicherndes und Orientierungshilfe bietendes Gegengewicht zu bilden. Dies gelte gerade in Zeiten vermehrten komplexen Informationsaufkommens einerseits und von einseitigen Darstellungen, Filterblasen, Fake News und Deep Fakes andererseits.

Aus dem vom BVerfG umrissenen Funktionsauftrag ist nach Auffassung der rbb-Datenschutzbeauftragten zumindest mittelbar auch der Auftrag abzuleiten, seine Angebote datenschutzfreundlich zu gestalten. Denn letztlich könnte eine Auswertung des Mediennutzungsverhaltens, die über das erforderliche Maß zur Gewinnung von Erkenntnissen zur zeitgemäßen und bedarfsgerechten Gestaltung von Angeboten hinausgeht, auch Möglichkeiten zur

Beeinflussung der Nutzer:innen eröffnen. Die öffentlich-rechtlichen Rundfunkanstalten bewegen sich hier in einem Spannungsverhältnis: Einerseits lautet ihr gesetzlicher Auftrag, soweit es zur Erreichung einer Zielgruppe aus journalistisch-redaktionellen Gründen geboten ist, Telemedien ggf. auch außerhalb eigener Portale anzubieten (vgl. § 30 Abs. 4 S. 2 i. V. m. § 33 Abs. 5 S. 2 MStV). Andererseits laufen sie durch ihre Präsenz auf den großen Social-Media-Plattformen außereuropäischer Anbieter Gefahr, in die datenschutzrechtliche Mitverantwortung für Datenverarbeitungsvorgänge, die nicht DSGVO-konform sind, zu geraten. In jedem Fall ist eine sorgfältige Einzelfallabwägung erforderlich. (Näheres dazu siehe Kap. C. V. 4.)

2.2 BGH-Urteile zu Ansprüchen gegenüber dem Betreiber eines sozialen Netzwerks, der unter dem Vorwurf der „Hassrede“ Beiträge gelöscht und Konten gesperrt hat

Der Bundesgerichtshof (BGH) hat mit zwei Urteilen vom 29.7.2021 die Geschäftsbedingungen von Facebook zur Löschung von Nutzerbeiträgen und Kontensperrung bei Verstößen gegen die in den Bedingungen festgelegten Kommunikationsstandards i. d. F. vom 19.4.2018 für unwirksam erklärt.

Zwar seien die Nutzungsbedingungen wirksam in das Vertragsverhältnis einbezogen worden, indem die Nutzer:innen auf die ihnen in Form eines Pop-up-Fensters zugegangene Mitteilung von Facebook über die beabsichtigte Änderung die entsprechende, mit „Ich stimme zu“ bezeichnete Schaltfläche anklicken mussten. Die Nutzungsbedingungen seien jedoch gemäß § 307 Abs. 1 Satz 1 BGB unwirksam, weil die Nutzer:innen des Netzwerks durch sie entgegen den Geboten von Treu und Glauben unangemessen benachteiligt werden. Grundsätzlich sei Facebook berechtigt, den Nutzer:innen die Einhaltung bestimmter Kommunikationsstandards vorzugeben, die über die strafrechtlichen Vorgaben hinausgehen. Facebook dürfe sich auch das Recht vorbehalten, bei Verstoß gegen die Kommunikationsstandards Beiträge zu entfernen und das betroffene Nutzerkonto zu sperren. Für einen interessengerechten Ausgleich der kollidierenden Grundrechte und damit die Wahrung der Angemessenheit sei es aber erforderlich, dass sich Facebook in seinen Geschäftsbedingungen verpflichtet, die Nutzer:innen über die Entfernung eines Beitrags zumindest nachträglich und über eine beabsichtigte Sperrung des Nutzerkontos vorab zu informieren, ihnen den Grund dafür mitzuteilen und eine Möglichkeit zur Gegenäußerung einzuräumen, an die sich eine Neubescheidung anschließt.

Die Konsequenzen dieser Entscheidung sind erheblich. Bis zur Neuschaffung eines Anhörungsverfahrens sind alle Äußerungen, die nicht strafbar sind, auf Facebook erlaubt. Nur das Strafrecht gilt unmittelbar als Maßstab für die Zulässigkeit von Äußerungen. Mit diesem Urteil wurde die Meinungsäußerungsfreiheit der Nutzer:innen von sozialen Plattformen gestärkt.

2.3 Urteil des BGH zur Facebook-Nutzung unter Pseudonym

In seinem Urteil vom 27.1.2022 hat der BGH entschieden, dass Facebook seinen Nutzer:innen grundsätzlich erlauben muss, Pseudonyme bei der Nutzung der Plattform zu verwenden. Die in den Nutzungsbedingungen von Facebook statuierte Klarnamenpflicht würde die Nutzer:innen entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Sie sei nicht mit dem Grundgedanken von § 13 Abs. 6 Satz 1 TMG (Anmerkung der Verf.: jetzt § 19 Abs. 2 TTDSG) zu vereinbaren, wonach Diensteanbieter die Nutzung der Telemedien anonym oder unter Pseudonym ermöglichen müssen, soweit dies technisch möglich und zumutbar ist.

2.4 Urteil des BGH zur Reichweite des Auskunftsanspruchs nach Art. 15 Abs. 1 DSGVO

Hinsichtlich der Reichweite des Auskunftsanspruchs nach Art. 15 Abs. 1 DSGVO gibt es zahlreiche nicht abschließend geklärte Rechtsfragen. Mit Urteil vom 15.6.2021 hat der BGH über die Reichweite des Auskunftsanspruchs eines Versicherungsnehmers gegen eine Versicherung entschieden. Das Urteil enthält einige grundsätzliche Feststellungen, die auch für den rbb als zur Auskunft Verpflichteter relevant sind:

Nach Ansicht des BGH ist der Auskunftsanspruch durch das Verlangen nach einer „vollständigen Datenauskunft“ hinreichend präzisiert und beschränke sich nicht auf Daten, die dem Betroffenen noch nicht bekannt seien. Auch die Kategorisierung als „interne Vermerke“ durch die datenverarbeitende Stelle stehe dem Auskunftsrecht nicht entgegen. Rechtliche Analysen könnten zwar personenbezogene Daten enthalten und unterfielen insoweit auch dem Auskunftsanspruch. Die auf ihrer Grundlage vorgenommene Beurteilung der Rechtslage selbst stelle jedoch keine Information über den Betroffenen dar.

Erfüllt i. S. v. § 362 Abs. 1 BGB sei ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang

darstellen. Wird eine Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftschuldners, dass die Auskunft vollständig ist.

2.5 Urteil des BAG zum Anspruch der Arbeitnehmer:innen auf Kopien von personenbezogenen Daten

Die DSGVO sieht in Art. 15 Abs. 3 einen Auskunftsanspruch vor, der u. a. Arbeitnehmer:innen als sogenannte betroffene Personen berechtigt, Kopien aller personenbezogenen Daten, die Gegenstand einer Verarbeitung beim Arbeitgeber sind, anzufordern. Umfang und Inhalt dieses Anspruchs sind bislang rechtlich umstritten. Am 27.4.2021 hatte das Bundesarbeitsgericht (BAG) erstmals über einen solchen Fall zu entscheiden. Der Arbeitnehmer hatte in seiner Klage pauschal die Vorlage sämtlicher E-Mail-Korrespondenz durch den ehemaligen Arbeitgeber verlangt, die mit oder über ihn durch Dritte geführt wurde. Das BAG hat die Grundsatzfrage, ob über einen Auskunftsanspruch nach Art. 15 Abs. 3 DSGVO die Herausgabe von Kopien – wie zum Beispiel ganzer Personalakten oder konkreter E-Mails – verlangt werden kann, offengelassen und die Klage schon wegen eines zu unbestimmten Klageantrags abgewiesen. Danach könne sich der Anspruch nicht auf eine unbestimmte Anzahl von E-Mails beziehen. Damit nach dem BAG ein Anspruch auf Vorlage bestimmter Unterlagen überhaupt in Betracht kommen kann, müsse sich das Begehren auf bestimmte Dokumente oder E-Mails konkretisieren. Anderenfalls könne ein entsprechendes Urteil gar nicht vollstreckt werden. Die weitere Entwicklung der Rechtsprechung zum Umfang des Auskunftsanspruchs bleibt abzuwarten. Liegt ein hinreichend konkretisierter Vorlage-Anspruch vor, der sich auf eine große Menge an Dokumenten erstreckt, ist es auf jeden Fall zulässig, dass der/die Arbeitgeber:in zunächst die Eingrenzung des Auskunftsersuchens unter Verweis auf den Erwägungsgrund 63 zur DSGVO verlangt.

III. Berlin/Brandenburg

Im Berichtszeitraum sind in Berlin/Brandenburg keine für den rbb datenschutzrelevanten Gesetze in Kraft getreten und auch keine datenschutzrelevanten Urteile erlassen worden.

IV. Wichtige Entscheidungen aus anderen Bundesländern

1. Urteil des Schleswig-Holsteinischen Oberverwaltungsgerichts zu den Facebook Fanpages

Der rbb verbreitet – wie alle anderen Rundfunkanstalten – seine Angebote auch über soziale Netzwerke wie Facebook, Instagram und Twitter. Bei der Nutzung der Drittplattformen findet ein umfangreiches Tracking des individuellen Nutzungsverhaltens durch die Plattformbetreiber statt. Ein besonderes Augenmerk in der Rechtsprechung und juristischen Diskussion liegt bislang auf der datenschutzrechtlichen Beurteilung der sogenannten Facebook Fanpages. Dabei handelt es sich um ein Dienstangebot von Facebook, mit dem sich Unternehmen auf der Plattform präsentieren können. Facebook stellt den Unternehmen dabei verschiedene Business-Tools zur Verfügung, u. a. insbesondere das Werkzeug „Facebook-Insights“. Damit können anonymisierte, nutzerbezogene Statistik-Informationen abgerufen werden. Die auf den Fanpages verfügbaren Inhalte können auch von Personen gelesen werden, die nicht bei Facebook registriert sind. Somit werden beim Aufruf einer Fanpage personenbezogene Daten sowohl registrierter als auch nicht registrierter Nutzer:innen verarbeitet. Technisch werden die „Insights“ mithilfe von Cookies generiert.

Das Schleswig-Holsteinische OVG hat nun einen seit mehr als zehn Jahren andauernden Rechtsstreit zu dieser Thematik mit Urteil vom 25.11.2021 beendet. Demnach war die durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) im Jahr 2011 angeordnete Deaktivierung der Facebook Fanpage gegenüber der Wirtschaftsakademie Schleswig-Holstein GmbH als Betreiberin einer Facebook Fanpage wegen mehrfacher schwerwiegender Datenschutzverstöße von Facebook im Zusammenhang mit dem Nutzertracking auf der Plattform rechtmäßig. Das ULD hatte seine Anordnung damit begründet, dass die

Nutzer:innen einer Facebook Fanpage nicht hinreichend entsprechend den Vorgaben des § 13 Abs. 1 TMG über die Erhebung und Verarbeitung ihrer personenbezogenen Daten informiert worden waren. Sie hätten in die Datenverarbeitung nicht wirksam eingewilligt. Außerdem beanstandete das ULD das Fehlen einer Widerspruchsmöglichkeit. Die registrierten Nutzer:innen seien nicht darüber informiert worden, dass die Informationen aus der Reichweitenanalyse mit ihren identifizierenden Angaben zusammengeführt wurden. Das ULD stellte ferner fest, dass die Wirtschaftsakademie Schleswig-Holstein GmbH als Fanpage-Betreiberin Dienstanbieterin und damit verantwortliche Stelle war.

In der Erstinstanz hatte das VG Schleswig die Untersagungsanordnung aufgehoben und dies damit begründet, dass Fanpage-Betreiber aufgrund mangelnder rechtlicher und tatsächlicher Möglichkeit der Einflussnahme keine verantwortliche Stelle seien. Diese Auffassung wurde in der Berufung vom Schleswig-Holsteinischen OVG im Jahre 2014 zunächst bestätigt. Dagegen legte das ULD Revision beim Bundesverwaltungsgericht (BVerwG) ein. Das BVerwG setzte das Verfahren aus und legte dem EuGH mehrere Fragen vor. Der EuGH hat daraufhin mit Urteil vom 5.6.2018 entschieden, dass Fanpage-Betreiber gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Nutzer:innen der Fanpage verantwortlich sind. Somit liege eine gemeinsame Haftung für Datenschutzverstöße vor. Unter Berücksichtigung der EuGH-Entscheidung urteilte das BVerwG am 11.9.2019, dass die Legaldefinition der verantwortlichen Stelle unionsrechtskonform auszulegen sei. Demnach sei verantwortlich, wer über die Zwecke und Mittel einer Datenverarbeitung (mit-)entscheidet. Unter Aufhebung des Berufungsurteils des Schleswig-Holsteinischen OVG aus dem Jahre 2014 wies es die Sache an das OVG zurück. Dabei gab es ihm auf zu prüfen, welche Datenerhebungen bei Aufruf der Fanpage im für die Entscheidung maßgeblichen Zeitpunkt stattfanden.

Mit Urteil vom 25.11.2021 hat das Schleswig-Holsteinische OVG daraufhin entschieden, dass die Deaktivierungsanordnung des ULD aus dem Jahre 2011 rechtmäßig erfolgt sei und die dagegen erhobene Klage abgewiesen. Maßgebliche Sach- und Rechtslage sei der Zeitpunkt der letzten Verwaltungsentscheidung, also des Widerspruchsbescheids vom 16.12.2011. Das OVG stellte schwerwiegende Verstöße gegen das Transparenzgebot fest, für die die Wirtschaftsakademie Schleswig-Holstein GmbH zumindest mitverantwortlich sei. Die Nutzer:innen seien nicht in ausreichender Weise über die Verarbeitungsvorgänge informiert worden. Die

verschiedenen Verarbeitungsschritte seien getrennt zu bewerten. Die Mitverantwortlichkeit der Fanpage-Betreiber bestehe insoweit nur für die Erstellung der „Facebook-Insight“-Statistik, hingegen nicht für die nachgelagerte Verknüpfung dieser Daten zur Erstellung von Profilen und zur Nutzung zu Werbezwecken. Die Mitverantwortlichkeit bei den „Insight“-Daten folge aus dem Umstand, dass erst durch die Einrichtung der Fanpage die Datenverarbeitung ermöglicht werde und diese hinsichtlich des Zielpublikums durch die Gestaltung der Fanpage gesteuert werde. „Gemeinsam“ (gemäß der vom EuGH am 5.6.2018 festgestellten „gemeinsamen Verantwortung“) sei nicht im Sinne einer gleichwertigen und gleichberechtigten Kontrolle jedes einzelnen Verarbeitungsschrittes zu verstehen, vielmehr könnten die Parteien unterschiedlich stark und in unterschiedlicher Weise in Entscheidungen eingebunden sein.

Die gemeinsame Verantwortlichkeit bei Facebook Fanpages ist nun abschließend geklärt. Daran ändert auch die Tatsache, dass mittlerweile die DSGVO Maßstab für die Beurteilung einer gemeinsamen Verantwortlichkeit ist, nichts. Die maßgeblichen Anforderungen gelten danach weiter fort. Die Fanpage-Betreiber sind schon aus dem Grund in der Mitverantwortung, dass sie mit der Einrichtung ihrer Fanpage die entsprechende Datenverarbeitung zur Nutzungsmessung ermöglichen und ihnen die Ergebnisse der Nutzungsmessung vom Plattformbetreiber zur Verfügung gestellt werden. Ein Beitrag der Fanpage-Betreiber zur Entscheidung über die Mittel der Datenverarbeitung liegt in dem Umstand, dass sie über die Gestaltung ihrer Fanpage entsprechend ihrem Zielpublikum (mit)steuern, wessen Daten erhoben und verarbeitet werden. Was die Zwecke der Verwendung von personenbezogenen Daten betrifft, ist entscheidend, dass die Datenverarbeitung zum Zweck der Erstellung von „Insight“-Statistiken den Betreibern im Ergebnis ermöglicht, Kenntnis über bestimmte Merkmale der Nutzer:innen der Fanpage zu erlangen, um ihnen relevantere Inhalte bereitstellen und Funktionen entwickeln zu können, die für sie von Interesse sein könnten. Durch Einrichtung der Fanpage entscheiden die Betreiber jedenfalls stillschweigend über den Zweck der insoweit maßgeblichen Datenverarbeitung mit.

Um die Konsequenzen aus dem Urteil für den rbb als Fanpage-Betreiber zu ermitteln, muss nun zunächst einmal geklärt werden, ob Facebook die vom OVG festgestellten Verstöße mittlerweile behoben hat. Problematisch ist in jedem Fall das Fehlen eines beidseitigen, ausgehandelten Joint-Controller-Vertrags nach Art. 26 DSGVO. Facebook stellt aktuell ein einseitig

gestelltes sogenanntes Addendum zur Verfügung. Dieses dürfte den Anforderungen des Art. 26 DSGVO nicht genügen. Dabei ist schon fraglich, ob eine einseitige Erklärung überhaupt den Anforderungen des Art. 26 DSGVO genügen kann. Jedenfalls sind die im Addendum gegebenen Informationen über die Datenverarbeitung nicht hinreichend aussagekräftig, um bewerten zu können, ob eine Verarbeitung auf einer Rechtsgrundlage aus Art. 6 DSGVO rechtskonform möglich ist. Ein weiteres Problem besteht in der Übermittlung der Nutzerdaten in die USA (s. dazu Kap. B. I. 4.).

Zu klären ist schließlich, ob und inwieweit sich die Grundsätze aus dem Urteil auf andere Drittplattformen wie Instagram oder Twitter übertragen lassen. Auch bei Instagram, das wie Facebook zu dem Unternehmen Meta Platforms gehört, stehen für Business-Profile umfassende Targeting-Optionen (z. B. Standort, demografische Daten, Interessen usw.) zur Verfügung. Ferner erfolgt eine Verknüpfung von Facebook Fanpages und Instagram, da Instagram voraussetzt, dass zuvor eine Facebook Fanpage erstellt wurde. Somit spricht einiges dafür, dass auch bei Instagram eine Mitverantwortung der Seiten-Betreiber gegeben ist. Bezüglich Twitter ist das juristische Meinungsbild noch deutlich gespaltener. Während die eine Auffassung eine Übertragbarkeit des EuGH-Urteils bejaht, da auch Twitter sogenannte „Insight"-Daten auswerte, ohne dass diese Funktion deaktiviert werden könne, sieht die Gegenauffassung keine Vergleichbarkeit, da – anders als bei Facebook – bei Twitter die Meinungs- und Informationsfreiheit anstatt einer kommerziellen Nutzung im Vordergrund stehe.

C. Datenschutz und Datensicherheit im rbb

I. Interne Regelungen

1. Allgemeines

Wie im letzten Tätigkeitsbericht dargelegt, muss das interne Regelwerk des rbb, das sogenannte rbb-Handbuch, inhaltlich überarbeitet und nutzerfreundlicher gestaltet werden. Das betrifft unter anderem die datenschutzrelevanten Regelungen. Auch muss dafür gesorgt

werden, dass sich alle verbindlichen Handlungsanweisungen für die Beschäftigten im rbb-Handbuch befinden und nicht nur an anderen Stellen im rbb-Intranet abrufbar sind, wie es aktuell z. B. für die Nutzungsbedingungen von Microsoft 365 der Fall ist (s. 17. Tätigkeitsbericht, S.31 ff.). Bislang bestand die Schwierigkeit der Umsetzung darin, dass die Zuständigkeiten für die einzelnen Regelungen dezentral verteilt sind und es keine Stelle im rbb gab, die die Gesamtheit der Regelungen und ihre Anordnung im rbb-Handbuch im Blick hat. Mit dieser Aufgabe hat die Intendantin Anfang 2022 mich in meiner Funktion als Compliance-Beauftragte betraut. Schritt für Schritt werde ich mich nun um die Aktualisierung, Vereinheitlichung und bessere Darstellung der Regelungen im rbb-Handbuch kümmern.

2. Dienstanweisung Informationsmanagement

Auf den Inhalt der Dienstanweisung (DA) Informationsmanagement, die seit Juni 2020 in Kraft ist, bin ich im letzten Tätigkeitsbericht ausführlich eingegangen (s. 17. Tätigkeitsbericht, S. 32 ff.). In ihr sind alle wesentlichen Anforderungen an die Verarbeitung von Daten und Informationen im rbb zusammengefasst. Die Regelungen dieser DA werden durch die Sicherheitsrichtlinien ergänzt, die der Informationssicherheitsbeauftragte nach Beratung im Informationssicherheitskreis auf Grundlage der DA Informationsmanagement erlässt. Diese Sicherheitsrichtlinien richten sich hauptsächlich an Betreiber und Beschaffer von IT-Systemen im rbb und sind auf Basis des BSI IT-Grundschutzes verfasst.

Weitere, über die DA Informationsmanagement hinausgehende, spezielle Regelungen zum Umgang mit personenbezogenen Daten finden sich in den Dienstvereinbarungen und Nutzungsbedingungen zu einzelnen IT-Systemen.

II. Arbeitsgruppen

1. Kreis der Datenschutz-Koordinator:innen

Das Datenschutz-Management des rbb sieht Datenschutz-Koordinatoren vor (Tz. 4.3 der Anlage 2 ‚Datenschutz' zur DA Informationsmanagement). Danach hat jede Direktion eine:n

Datenschutz-Koordinator:in benannt. Zusätzlich hat auch die Intendanz eine Datenschutz-Koordinatorin bestellt. Die Datenschutz-Koordinator:innen stellen das Bindeglied zwischen der Datenschutzbeauftragten und der jeweiligen Direktion dar.

Im Berichtszeitraum gab es zwei Treffen der Datenschutz-Koordinator:innen per Videokonferenz, an denen jeweils auch ein:e Vertreter:in aus den unter der Federführung des rbb stehenden ARD-Gemeinschaftseinrichtungen (GSEA) ARD-Hauptstadtstudio, ARD Play-Out-Center, ARD-Text, Informations-Verarbeitungs-Zentrum und ARD-Generalsekretariat teilgenommen hat.

In der Videokonferenz vom 22.6.2021 wurden folgende Themen behandelt:

- Konsequenzen für den rbb aus dem Urteil des EuGH vom 16.7.2020 zur Unwirksamkeit des Privacy Shield („Schrems II“),
- neue Standardvertragsklauseln der EU-Kommission vom 4.6.2021,
- TTDSG,
- rbb-Nutzungsbedingungen für Microsoft 365,
- Neuregelung für inaktive IT-Benutzerkonten in Microsoft 365,
- Stand des VVT,
- Abgrenzung der Rollen Informationstreuhänder/Informationsverantwortlicher,
- Workflow im Zusammenhang mit der Bearbeitung von datenschutzrechtlichen Auskunftsersuchen und
- Bedeutung und Reichweite des Medienprivilegs.

In der Videokonferenz vom 17.12.2021 haben wir uns u. a. mit folgenden Themen beschäftigt:

- Beschaffungsvorgänge und Datenschutz,
- Abgrenzung Auftragsverarbeitung/Joint Controlling,

- Einzelfragen im Zusammenhang mit den neuen Standardvertragsklauseln,
- Vereinbarungen nach Art. 26 DSGVO für die Gemeinschaftseinrichtungen,
- Einzelfragen im Zusammenhang mit der Auslegung des TTDSG und
- Reichweite und Umfang des datenschutzrechtlichen Rechts auf Auskunft.

Die Datenschutz-Koordinator:innen sind ausnahmslos offen für die Themen Datenschutz und Informationssicherheit und nehmen die von mir gegebenen Informationen interessiert auf. Allerdings muss die Zusammenarbeit noch weiter intensiviert werden. Wichtig ist ein kontinuierlicher Austausch zwischen dem/der jeweiligen Datenschutz-Koordinator:in und der Datenschutzbeauftragten über datenschutzrechtlich relevante Vorhaben in der jeweiligen Direktion. Die in der DA Informationsmanagement vorgesehene Unterstützung der Fachbereiche bei der Erstellung der Dokumente für die Meldung von Verfahren zum VVT durch die Datenschutz-Koordinator:innen findet bislang nur vereinzelt statt. Der Grund dürfte darin liegen, dass die Datenschutz-Koordinator:innen diese Aufgaben zusätzlich zu ihrer Haupttätigkeit erledigen müssen. Solange es keine klare Regelung über die zur Verfügung stehende Zeit für dieses Amt gibt, besteht die Gefahr, dass die Aufgaben als Datenschutz-Koordinator:in immer zu kurz kommen. Problematisch ist auch, dass noch nicht alle Direktionen eine Vertretung für ihre:n Datenschutz-Koordinator:in benannt haben.

⇨ Notwendig ist eine verbindliche Regelung über das den Datenschutz-Koordinator:innen zur Verfügung stehende Zeitkontingent.

⇨ Notwendig ist eine Vertretungsregelung für die Datenschutz-Koordinator:innen.

2. Informationssicherheitskreis

Der Informationssicherheitsbeauftragte leitet gemäß der DA Informationsmanagement den Informationssicherheitskreis, deren Mitglied die Datenschutzbeauftragte ist. Im Berichtszeitraum hat der Informationssicherheitskreis am 29.10.2021 per Videokonferenz getagt. In dem Termin haben wir uns erstmals mit dem neuen Notfallmanagement des rbb beschäftigt. Die wesentlichen Punkte sollen als neue Anlage 12 in die DA Informationsmanagement

aufgenommen werden. Die Arbeit an der Anlage dauert noch an. Zusammen mit anderen inzwischen notwendigen Anpassungen der DA Informationsmanagement werden der Informationssicherheitsbeauftragte und ich sie voraussichtlich im Frühsommer 2022 nach einer gemeinsamen finalen Abstimmung im Informationssicherheitskreis und im Kreis der Datenschutz-Koordinator:innen der Geschäftsleitung zur Beschlussfassung vorlegen.

III. Bereichsübergreifende IT-Projekte/-Anwendungen

1. SAP-Prozessharmonisierung – Projekt „(D)ein SAP“

Über den Stand des ARD-Projekts „(D)ein SAP“ hatte ich zuletzt in meinem 17. Tätigkeitsbericht (S. 36 ff.) informiert.

Die datenschutzrechtliche Prüfung des neuen SAP-Systems erfolgt für die einzelnen Module in den Rundfunkanstalten nach dem Federführungsprinzip durch die jeweiligen Datenschutzbeauftragten. Meine Federführung betrifft das vom rbb als Prozesseigner verantwortete Modul ‚Beschaffung/Vertragswesen/Warenwirtschaft‘. In diesem Zusammenhang hatte ich an der Erarbeitung der datenschutzrelevanten Anforderungen und Dokumente für die EU-Ausschreibung eines Cloud-Services (‚Software as a Service‘) für das E-Procurement (elektronische Bedarfsanmeldung von Handelswaren und Dienstleistungen) mitgewirkt. Nachdem der erste Zuschlag hierfür aufgehoben werden musste, konnte er inzwischen – nach vorheriger datenschutzrechtlicher Prüfung des Angebots durch den AK DSB – an den zweitplatzierten Bieter erteilt werden.

Wie berichtet, hatte ich alle vom Projekt für die Integrationstests des Moduls ‚Beschaffung/Vertragswesen/Warenwirtschaft‘ mit Echtdaten vorgelegten Unterlagen geprüft und – wie auch meine Kolleg:innen für die anderen Module – umfangreiche Anmerkungen an die Projektleitung zurückgemeldet. Daraus hatte diese sogenannte Aufgaben-Backlogs erstellt, die im Berichtszeitraum Schritt für Schritt vom Projektteam abgearbeitet wurden. Nach aktuellem Stand sollen die Tests mit Echtdaten (Integrationstest, Anwenderakzeptanztest, Generalprobe) zum 1.6.2022 starten. Die dazu vorgelegten aktualisierten Dokumente habe ich geprüft und für plausibel erklärt.

Ferner habe ich mich im Berichtzeitraum noch mit den Sicherheits-Logdaten im SAP Security Audit Log (SAL) beschäftigt. Das SAL protokolliert alle sicherheitsrelevanten Vorfälle. Zweck der Speicherung ist die Aufklärung von technischen Problemen bzw. Sicherheitsvorfällen. Das SAL wird zunächst für den SAP Solution Manager aktiviert. Der Solution Manager ist das zentrale Tool, mit dem alle Anwendungen innerhalb „(D)ein SAP“ über ihre gesamte Lebensdauer hinweg von der Entwicklung über die Testung bis zum Betrieb und danach zur Weiterentwicklung gesteuert und dokumentiert werden. Später wird es als einheitliche Funktion in allen Systemen aktiviert. Nachdem der Projektleiter in Abstimmung mit mir angemessene Löschfristen für das SAL definiert hat, habe ich dem AK DSB empfohlen, der Einführung des SAL zuzustimmen, was erfolgt ist.

2. Microsoft 365

Wie berichtet, nutzt der rbb die Kommunikations- und Kollaborationsplattform Microsoft 365. Zu den grundsätzlichen datenschutzrechtlichen Bedenken verweise ich auf die Ausführungen in meinen früheren Tätigkeitsberichten (zuletzt im 17. Tätigkeitsbericht, S. 34 ff.)

Auch im Berichtsjahr hat die AG Microsoft 365, der Mitarbeiter:innen der HA Mediensysteme und IT (HA MIT), Mitglieder des Personalrats, ein Vertreter der Hauptabteilung (HA) Personal, die Schwerbehindertenvertretung, der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte angehören, mindestens einmal im Monat per Videokonferenz getagt und für die vom rbb vorgesehenen Erweiterungen des Systems Rahmenbedingungen definiert. Daneben hat uns die HA MIT regelmäßig per Newsletter über die von Microsoft einseitig vorgenommenen Änderungen am System informiert.

Aufgrund der Zunahme von Cyberangriffen ist der rbb Empfehlungen des BSI gefolgt und hat – wie von der AG Microsoft empfohlen – den Schutz für die Benutzerkonten erhöht: Während die sogenannte Multi-Faktor-Authentifizierung bislang nur bei einem Zugriff auf die Dienste von Microsoft von außerhalb des rbb-Netzwerkes (bspw. aus dem Homeoffice) oder mit rbb-fremden Geräten (bspw. mit privaten Smartphones) verlangt wurde, ist sie nun in allen Fällen der Nutzung von rbb-Accounts verpflichtend. Zudem wurde beschlossen, inaktive Gast-Benutzerkonten zukünftig nach einer kurzen Frist zu löschen. Bislang erfolgte für diese Konten –

anders als für inaktive rbb-Benutzerkonten – keine automatische Löschung. Dass solche Konten ein Sicherheitsrisiko waren, liegt auf der Hand. Sie hätten unbemerkt angegriffen werden können.

Schon in meinem letzten Tätigkeitsbericht hatte ich darauf hingewiesen, dass das ursprüngliche Sicherheitskonzept für Microsoft 365 überarbeitet werden muss (s. 17. Tätigkeitsbericht, S. 35). Das betrifft insbesondere den Versand von E-Mails mit vertraulichem Inhalt. Klassifiziert man E-Mails als „vertraulich“, so können sie mit ggf. angehängten Office-Dokumenten bislang nur von dem/der direkt genannten Empfänger:in gelesen und bearbeitet werden. Diese rigiden Schutzmechanismen passen nicht zu den Arbeitsweisen innerhalb des rbb. Eine Veränderung des Sicherheitskonzepts unter Beibehaltung des hohen Schutzniveaus und Nutzerkomforts konnte im Berichtsjahr nicht erreicht werden. Die ursprünglich nur als Übergangslösung aufgezeigte Möglichkeit, E-Mails mit vertraulichem Inhalt manuell zu verschlüsseln, soll laut HA MIT nun wohl dauerhaft praktiziert werden. Dies ist umständlich und birgt die Gefahr, dass im Eilfall von den Anwender:innen auf jegliche Sicherheitsmaßnahme verzichtet wird.

- ⇨ Es bleibt zu hoffen, dass doch noch eine einfachere und nutzerfreundlichere Lösung entwickelt werden kann – gegebenenfalls im ARD-Verbund.

3. IT-Sicherheitslösung SIEM/SOC

Zur Erfüllung ihres gesetzlichen Auftrages nutzen die öffentlich-rechtlichen Rundfunkanstalten in Deutschland umfangreiche IT-Infrastrukturen sowohl für die redaktionelle Arbeit als auch für die Produktion und Distribution von Medienangeboten. Der Schutz der IT-Infrastrukturen vor Angriffen durch Dritte gewinnt stetig an Bedeutung. Das BSI bestätigt für den Bereich Medien und insbesondere für den öffentlich-rechtlichen Rundfunk ein hohes Gefährdungspotential durch eine stetig steigende Bedrohungslage.

Um professionelle Cyberangriffe erkennen zu können, sind Systeme notwendig, die über eine Analyse der vielfach anfallenden Log- und Protokolldaten Abweichungen vom Normalverhalten der Systeme erkennen können. Die Auswertung dieser Log- und Protokolldaten, die Definition der Normwerte und Systemcharakteristika sowie die Alarmierung erfolgt durch sogenannte SIEM-Tools (SIEM steht für Security Information und Event Management).

Diese sehr leistungsfähigen Werkzeuge zur Erhöhung der IT-Sicherheit können ihre volle Wirksamkeit nur dann entfalten, wenn sie qualifiziert betreut und betrieben werden und die Log- und Protokolldaten regelmäßig und umfassend ausgewertet werden. Dies geschieht in einem sogenannten Security Operation Center (SOC). Die zuständigen ARD-Gremien haben sich im Frühjahr 2022 auf eine dauerhafte, gemeinschaftliche und leistungsstarke Lösung mittels der Kombination aus SIEM und SOC verständigt. Danach wird eine zentrale Infrastruktur auf Basis von SIEM/SOC beim ARD-Sternpunkt aufgebaut. Der ARD-Sternpunkt ist beauftragt, eine entsprechende Lösung für die ARD zu beschaffen und zu betreiben. Für den AK DSB wird die Angelegenheit von der stellvertretenden Datenschutzbeauftragten des HR begleitet. Sie achtet u. a. darauf, dass die notwendigen Festlegungen zu IT-Sicherheit und Datenschutz in die Vergabe-Unterlagen aufgenommen werden. Außerdem wirkt sie an der DSFA für die SIEM/SOC-Systeme mit und achtet auf den Abschluss der notwendigen Verträge zur Auftragsverarbeitung. Die Kollegin berichtet kontinuierlich über den Stand des Projektes und stimmt sich mit den übrigen Mitgliedern des AK DSB ab.

4. Neues Besucheranmeldesystem

Wie berichtet (zuletzt im 17. Tätigkeitsbericht, S. 42 f.), hat der rbb das Verfahren für die Anmeldung von Besucher:innen, Auszubildenden, Praktikant:innen und neuen Mitarbeiter:innen neu gestaltet. Mit Hilfe eines browserbasierten Tools können Informationen über zutrittsberechtigte Personen mit einer standardisierten Anmeldung per Intranet an die Empfänge übermittelt werden. Nach einem mehrjährigen Probebetrieb konnte das Verfahren im August 2021 mit Zustimmung der Datenschutzbeauftragten in den Regelbetrieb gehen.

IV. Beschäftigtendatenschutz

1. Datenschutzfragen im Zusammenhang mit den coronabedingten Maßnahmen

Auch im Berichtsjahr haben mich wieder viele Einzelfragen im Zusammenhang mit der Umsetzung der Infektionsschutzverordnungen von Berlin und Brandenburg beschäftigt.

Als eines der ersten Unternehmen hat der rbb seit Februar 2021 seinen Beschäftigten Corona-Selbsttests unter medizinischer Aufsicht angeboten. Die TOM zum Datenschutz in diesem Zusammenhang hatte die HA Personal zuvor mit mir gemeinsam festgelegt und im weiteren Verlauf mehrmals nachgeschärft. Die Arbeit des medizinischen Dienstes erfolgte auf der Basis eines Vertrags zur Auftragsdatenverarbeitung.

Hervorzuheben ist auch die datenschutzkonforme Umsetzung des 3G-Nachweises am Arbeitsplatz in der Zeit vom 24.11.2021 bis 31.3.2022. Wie in den meisten anderen Rundfunkanstalten wurde die strikte 3G-Pflicht umgesetzt, indem die Schranken- und Türen-Öffnungsfunktion auf allen rbb-Hausausweisen abgeschaltet und erst freigeschaltet wurde, nachdem ein entsprechender Nachweis (2-G = geimpft oder genesen) erbracht worden war. Die Beschäftigten mussten an den Eingängen ein gültiges 3G-Zertifikat in Verbindung mit einem Lichtbildausweis vorweisen. Wer diese Kontrolle einmal absolviert hatte, konnte weitere vermeiden, indem der eigene Status (entweder geimpft oder genesen) dauerhaft im Hausausweis-System hinterlegt wurde. Dies konnte entweder über speziell dafür eingerichtete Counter an den Standorten des rbb, aber auch auf elektronischem Wege geschehen. Das zunächst dafür vorgesehene Verfahren mit Unterstützung von Microsoft Forms habe ich abgelehnt. Statt dessen kam für die Übermittlung des Status zunächst die rundfunkeigene ARD/ZDF-Box zum Einsatz. Auf freiwilliger Basis konnten die Kolleg:innen ihren Impf- bzw. Genesenen-Nachweis in die ARD/ZDF-Box hochladen. Ein kleiner Kreis von Mitarbeiter:innen der Abteilung Infrastruktur prüfte sodann die auf diese Weise übermittelten Dokumente mit der CovPassCheck-App. Danach wurde ein entsprechender Eintrag im Hausausweis-System vorgenommen und die Dokumente in der ARD/ZDF-Box unverzüglich gelöscht. Nachdem ab Februar 2022 aufgrund geltender EU-Bestimmungen digitale Impfzertifikate ohne Booster-Impfung nur noch bis zu neun Monate gültig waren, sich zusätzlich die Voraussetzungen für eine Grundimmunisierung mit dem Johnson & Johnson-Impfstoff geändert hatten und auch der Genesenen-Status eine veränderte Gültigkeit bekommen hatte, musste eine neue, erweiterte Meldung im Hausausweissystem vorgenommen werden. Um den personellen Aufwand hierfür so gering wie möglich zu halten, haben die Teams der Abteilung Infrastruktur und der HA MIT in enger Abstimmung mit der Datenschutzbeauftragten einen Selfservice entwickelt. Jede:r Beschäftigte konnte danach selbst das Impfzertifikat validieren und den Impfstatus sowie den Zeitpunkt der Impfung speichern und somit den Zugang mit dem Hausausweis automatisch freischalten bzw. verlängern.

Dafür musste nur der Code des Impfzertifikats per Webcam eingescannt werden. Alternativ konnte ein Screenshot des Codes hochgeladen werden.

Die Tatsache, dass der rbb innerhalb der HA MIT Mitarbeiter:innen beschäftigt, die in der Lage sind, solche Funktionen unter hohem Zeitdruck als Eigenentwicklung zu programmieren, ist von großem Vorteil und trägt zu der Wahrung einer gewissen Unabhängigkeit von den großen Tech-Unternehmen bei. Da diese Expert:innen außerdem eine besondere Sensibilität für das Thema Datenschutz haben, ist die Zusammenarbeit mit ihnen für mich besonders erfreulich.

2. SAP xSS-Anwendung

In meinen zurückliegenden Tätigkeitsberichten hatte ich über die probeweise Einführung der SAP xSS-Anwendungen „An- und Abwesenheitsmanagement“ (seit 2.9.2019) und „Meine Entgeltnachweise“ (seit 1.6.2020) berichtet (s. 17. Tätigkeitsbericht, S. 45). Der Probebetrieb wurde dazu genutzt, praktische Erfahrungen zu sammeln, technische Probleme zu beheben und Verbesserungen vorzunehmen. Mit Zustimmung des Personalrats konnten die Anwendungen am 1.2.2022 in den Regelbetrieb gehen.

3. Digitalisierung der Personalakten

Wie im 17. Tätigkeitsbericht (S. 48 f.) mitgeteilt, wird der rbb die Personal- und Vorgangsakten für freie Mitarbeiter:innen künftig in digitaler Form führen. Nur noch einige wenige Papier-Dokumente werden im Original aufbewahrt werden. Das Dokumentenmanagement-System zur Aufbewahrung der digitalen Akten soll in das existierende SAP-System integriert werden.

Mit der Digitalisierung der Akten hat der rbb ein Berliner Unternehmen beauftragt, dessen Sicherheitskonzept für den Umgang mit den Akten bei dem Transport, der Lagerung und der Verarbeitung dem sehr hohen Schutzbedarf der Personalakten entspricht. Es handelt sich dabei um denselben Dienstleister, der auch schon die Akten der Abteilung Lizenzen digitalisiert hat. Am 20.12.2021 habe ich das Verladen der Vorgangsakten der freien Mitarbeiter:innen durch den Dienstleister am derzeitigen Sitz der HA Personal am City Campus Berlin beaufsichtigt. Den Prozess des Ausladens und der Weiterverarbeitung beim Dienstleister vor Ort in Treptow hat in enger Abstimmung mit mir der verantwortliche Mitarbeiter der HA MIT

kontrolliert. Er wurde dort vom Berliner Standortleiter und dem externen Datenschutzbeauftragten der Firma empfangen. Der Kollege aus der HA MIT hat die Einhaltung der vertraglich zugesicherten TOM im Einzelnen überprüft. Nachdem keine Mängel festgestellt worden waren, konnte das Audit erfolgreich abgeschlossen werden.

Die eigentliche Aktenführung im neuen Dokumentenmanagement-System muss noch mit mir abgestimmt werden. Dafür wird auch eine Anpassung der Dienstanweisung zur Führung der Personalakten erforderlich sein.

4. Arbeitsunfallmeldungen

Arbeitsunfälle müssen u. a. aus Versicherungsgründen gemeldet werden. Zu unterscheiden sind zwei unterschiedliche Arten von Meldungen: die Arbeitsunfallmeldung gemäß § 193 Siebtes Buch Sozialgesetzbuch – Gesetzliche Unfallversicherung (SGB VII) – und die Erste-Hilfe-Meldungen gemäß § 24 Abs. 6 Deutsche Gesetzliche Unfallversicherung (DGUV), Vorschrift 1. Verarbeitet werden in diesem Zusammenhang u. a. auch besonders geschützte personenbezogene (Gesundheits-)Daten. Im Berichtszeitraum habe ich mich eingehend mit dem bisherigen Meldeverfahren beschäftigt. Mit Unterstützung einer Mitarbeiterin der HA Personal haben der Sicherheitsingenieur und seine Mitarbeiterin entsprechend meinen Vorgaben den Workflow für beide Meldungen optimiert, indem der Kreis der Meldeempfänger:innen und die Aufbewahrungsfristen verkürzt wurden. Außerdem wurden das Dokument „Arbeits- und Wegeunfall – Fragen und Antworten“ und die Datenschutzerklärungen an die neuen Workflows angepasst. Nach Abschluss der Arbeiten konnte ich die beiden Verfahren „Unfallanzeigen“ und „Erste-Hilfe-Meldungen“ in das VVT aufnehmen.

5. Datenverarbeitung im Auszubildendenverhältnis

Um das mit den Auszubildenden begründete Beschäftigungsverhältnis durchführen und eine erfolgreiche Ausbildung gewährleisten zu können, muss der rbb an mehreren Stellen personenbezogene Daten der Auszubildenden verarbeiten. Neben der HA Personal und der ausbildenden Fachabteilung verarbeitet auch die HA MIT Daten der Auszubildenden, um ihnen die erforderliche Hard- und Software zur Verfügung stellen zu können. Im Rahmen der Anmeldung zum Berufsschulunterricht gibt der rbb Daten der Auszubildenden an die zuständige

Berufsschule weiter. Die IHK erhält vom rbb personenbezogene Daten der Auszubildenden, um den Ausbildungsvertrag in das Ausbildungsverzeichnis eintragen zu können. Zur Herstellung einer größtmöglichen Transparenz über die Verarbeitung ihrer personenbezogenen Daten durch den rbb erhalten die Auszubildenden seit 2021 neben der allgemeinen Datenschutzerklärung der HA Personal zusätzliche eine speziell auf sie zugeschnittene Datenschutzerklärung. Diese hat die HA Personal gemeinsam mit mir ausgearbeitet.
Da auch im Jahr 2021 aufgrund der coronabedingten Abstandsregelungen kein gemeinsames Gruppenfoto von den neuen Auszubildenden für das Intranet erstellt werden konnte, hat die HA Personal ihnen angeboten, einen „Steckbrief“ mit ihren persönlichen Informationen im Intranet zu veröffentlichen. Auf der Basis einer ausführlichen Information über den Zweck des Steckbriefs und dessen Freiwilligkeit hat die HA Personal entsprechende Einwilligungen von den Auszubildenden für eine einwöchige Veröffentlichung der Steckbriefe im Intranet eingeholt. Das Verfahren wurde zuvor mit mir abgestimmt.

Wegen der rechtlichen Rahmenbedingungen für eine geplante Veröffentlichung von Namen, Fotos, Video- und Audioaufnahmen der Auszubildenden auf einem Azubi-Instagram-Kanal habe ich die HA Personal an das Justitiariat verwiesen, da in diesem Fall das allgemeine Persönlichkeits- und das Urheberrecht zur Anwendung kommt.

6. Gebäudemanagement-System

Die Hauptabteilung Gebäudemanagement (HA GM) nutzt seit mehreren Jahren ein IT-Produkt der Speedikon Facility Management AG zur Unterstützung beim Gebäudemanagement, das Computer-Aided Facility Management (CAFM). Das System wird von der HA MIT betrieben. Den externen Support leistet der Hersteller. Der rbb hat mit der Firma einen entsprechenden Vertrag zur Auftragsverarbeitung geschlossen und nutzt folgende Funktionen:

- Verwaltung von Raumplänen
- Störungsmanagement (Ticketsystem der HA GM)
- Zusammenarbeit mit externen Dienstleistern
- Buchung von Konferenzräumen

- Zuordnung von Personal zu Räumen
- Flächenverwaltung der rbb-Liegenschaften
- Dokumenten- und Vertragsverwaltung

Inzwischen hat der Hersteller sein Produkt auf einer neuen Basis weiterentwickelt und bietet weitere Funktionsmodule an. Die neue Plattform trägt den Namen Speedikon C. Die HA GM plant den Einsatz dieser weiterentwickelten Software für folgende neue Verfahren:

- Arbeitsplatzreservierung
- Schlüsselverwaltung

Der Hintergrund des Verfahrens „Arbeitsplatzreservierung“ ist die Tatsache, dass die Möglichkeit zur mobilen Arbeit im rbb auch nach dem Ende der Corona-Pandemie weiter bestehen wird. Über die genauen Konditionen führt der rbb zurzeit Tarifverhandlungen mit den Gewerkschaften. Um auch schon bis zum Abschluss der Tarifverhandlungen mobile Arbeit im rbb zu ermöglichen, hat die Geschäftsleitung eine Richtlinie für die mobile Arbeit beschlossen, die ab 1.5.2022 bis zum Abschluss eines Tarifvertrages gelten wird. Die Beibehaltung der Möglichkeit zur mobilen Arbeit führt zu einer Reduzierung des Raumbedarfs innerhalb des rbb. Aktuell werden von der HA GM neue Raumkonzepte erarbeitet, die vorsehen, dass nicht mehr jede:r Mitarbeiter:in einen eigenen Arbeitsplatz im rbb hat. Daher wird in Zukunft ein Arbeitsplatzreservierungssystem erforderlich sein, mit dem sich die Beschäftigten für bestimmte Zeiten einen Arbeitsplatz innerhalb des rbb reservieren können. Die Konfiguration des Systems wurde mit mir abgestimmt. Danach kann die buchende Person – mit Ausnahme des jeweils aktuellen Tages – nur ihre eigenen Buchungen einsehen; sie hat nicht die Möglichkeit, Buchungen aus der Vergangenheit einzusehen oder solche weiter als vier Wochen im Voraus vorzunehmen. Das System gibt allerdings stichtagbezogen Auskunft darüber, welche Kolleg:innen zur selben Zeit einen Arbeitsplatz gebucht haben, um ggf. gemeinsame Arbeitsräume schaffen zu können. Über das Beschriebene hinaus ist auch den Vorgesetzten keine weitergehende Einsicht möglich. Die Buchungsdaten werden nach drei Monaten anonymisiert und nach zwölf Monaten gelöscht.

Das Modul „Schlüsselverwaltung“ dient der elektronischen Erfassung der Schlüsselaus- und rückgaben. Eine Auswertung über die Häufigkeit und/oder Dauer des Zutritts zu Räumen ist nicht möglich. Einsicht in die beim Schließmanagement verarbeiteten Daten hat ausschließlich die Abteilung Infrastruktur zum Zweck des Vermerks der Ausgaben/Rücknahmen. Die Daten im Schließmanagement werden zwölf Monate nach Ausscheiden der einzelnen Mitarbeitenden anonymisiert.

Nachdem die für beide Verfahren für das VVT erforderlichen Dokumente gemeinsam erarbeitet waren, konnten sie in das VVT aufgenommen werden. Mittelfristig ist laut HA GM die vollständige Ablösung des alten Systems (Speedikon FM) geplant. Die Aufnahme der weiteren Funktionen/Verfahren ins VVT wird im Zuge dieser Umstellung erfolgen.

7. Dispositionssysteme

Zur Disposition von Personal und Sachmitteln für Produktionen werden im rbb weiterhin unterschiedliche Systeme genutzt. Keines der Systeme konnte bislang in das VVT aufgenommen werden. Ein Grund dafür ist, dass bislang keines der verwendeten Systeme vollständig datenschutzkonform ist (s. dazu auch 17. Tätigkeitsbericht, S. 46). Das Dispositionssystem MIRAAN ist schon seit Jahren im Einsatz, obwohl es bislang keine Programme zum erforderlichen automatischen Löschen von Dispositionsdaten gegeben hat. Außerdem fehlt eine Funktion zur Verkürzung der Sichtbarkeit von Dienstplan-Daten. Vor kurzem hat mir die verantwortliche Mitarbeiterin der HA MIT auf Nachfrage mitgeteilt, dass die technische Löschroutine inzwischen vom Hersteller umgesetzt sei. Auch eine Verkürzung der Sichtbarkeit der Dienstplan-Daten sei beim Hersteller beauftragt. Es wurde zugesagt, dass bis Ende Juni 2022 alle notwendigen Dokumente für die Aufnahme im VVT vorliegen.

In der Hörfunk-Disposition wird nach wie vor das völlig veraltete Dispositionssystem MaLu eingesetzt. In meinem letzten Tätigkeitsbericht hatte ich darauf hingewiesen, dass es für dieses System bislang kein Löschkonzept gibt. Das Berechtigungskonzept ist fehlerhaft und die technischen Auswertungsmöglichkeiten gehen zu weit. Wegen der nach wie vor existierenden Probleme bei MIRAAN konnte das System MaLu bis heute nicht – wie geplant – durch MIRAAN

abgelöst werden. Die verantwortliche Mitarbeiterin der HA MIT hat mir versichert, das Ziel, MaLu so schnell wie möglich abzulösen, weiter zu verfolgen.

8. rbb Forms

Zur Ablösung einfacher Papierformulare und damit verbundener Genehmigungsworkflows haben Mitarbeiter der HA MIT die Applikation „rbb Forms“ entwickelt. Mit dieser Applikation sollen möglichst 90% der aktuellen Papierformulare abgelöst und deren Arbeitsschritte digital durchgeführt werden. Mit dieser Eigenentwicklung ist es den Fachbereichen möglich, selbst entsprechende Formulare auf einfache Weise zu erstellen. Sie erhalten dazu eine Oberfläche mit einer Reihe von Eingabefeldern. Um die automatische Eingabe zu unterstützen, werden auch Daten aus anderen Systemen genutzt. Die Applikation unterstützt die Fachbereiche auch bei der Erstellung der für jedes Antragsformular erforderlichen Datenschutzerklärung, indem entsprechende – mit mir abgestimmte – Vorlagen dafür bereitgestellt werden. Jedes neu erstellte Formular wird zudem von mir geprüft, bevor es zur Nutzung freigegeben werden kann. Das System wird von der HA MIT selbst betrieben. Im August 2021 startete der bis zum 18.2.2022 befristete Probebetrieb. Nachdem sich das System im Probebetrieb bewährt hat, ist es mit der Zustimmung aller Gremien im März 2022 in den Regelbetrieb gegangen.

V. Datenschutz bei der Produktion und im Programm

1. Entwicklung eines „Digital Interview Akquise Systems“

Aufgrund der coronabedingten Abstandsregelungen wurden in den vergangenen beiden Jahren vermehrt Interviews per Internet durchgeführt. Dabei wurden verschiedene Konferenzsysteme wie Skype, Teams, Zoom, Facetime usw. eingesetzt, die zum Teil nicht den datenschutzrechtlichen Standards des öffentlich-rechtlichen Rundfunks entsprechen. Außerdem sind diese Systeme im Kern für die Durchführung von Schalt-Konferenzen ausgelegt, unterstützen aber nicht die weitere Bearbeitung entstehender Audio- und Videodaten. Die bisherigen Lösungen sollen mit einem eigenen, auf die spezifischen Anforderungen zugeschnittenen

Tool abgelöst und verbessert werden. In Kooperation mit anderen öffentlich-rechtlichen Rundfunkanstalten wird das Tool derzeit entwickelt. Damit es den sich rasant weiterentwickelnden Technologiefortschritten zukünftig folgen kann, wird das System auf Basis eines Open-Source-Produkts entwickelt. Das Hosting soll zentral für alle kooperierenden Rundfunkanstalten erfolgen und das Tool als Clouddienst vom rundfunkeigenen Informationsverarbeitungszentrum (IVZ) zur Verfügung gestellt werden. Die rbb-Projektleitung bindet die Datenschutzbeauftragte und den Informationssicherheitsbeauftragten eng in die einzelnen Entwicklungsschritte ein. Sobald ein vorläufiges Betriebskonzept vorliegt, wird dieses auch den Datenschutzbeauftragten der anderen Kooperationspartner präsentiert.

2. KI-Projekte

Künstliche Intelligenz (KI) gewinnt bei der Produktion redaktioneller Inhalte zunehmend an Bedeutung (s. dazu 17. Tätigkeitsbericht, S. 49 ff.). In der Abteilung Technisches Innovationsmanagement (TIM) werden derzeit insgesamt sechs KI-Projekte durchgeführt, bei denen zum Teil auch biometrische Daten verarbeitet werden. So ermöglicht die Auswertung biometrischer Bilddaten mittels KI eine automatische Zuordnung von Bildern von Personen des öffentlichen Lebens zu deren Namen. Diese Technologie kann sowohl bei der Archivierung als auch bei der Produktion neuer Inhalte eingesetzt werden.

Im Berichtszeitraum hat sich die Datenschutzbeauftragte einmal grundsätzlich mit den datenschutzrechtlichen Rahmenbedingungen beim Einsatz von KI für journalistisch-redaktionelle Zwecke auseinandergesetzt, wobei der Schwerpunkt auf der Prüfung der rechtlichen Zulässigkeit des Einsatzes von KI unter Verwendung biometrischer Daten lag. In der DSGVO werden biometrische Daten als besonders sensible Daten angesehen. Sie unterliegen daher einem besonderen Schutz. Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person grundsätzlich untersagt, soweit nicht ein Ausnahmetatbestand des Art. 9 Abs. 2 DSGVO einschlägig ist. Für die Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen Zwecken gilt das Medienprivileg. Danach finden Teile der Vorschriften der DSGVO für die Verarbeitung zu journalistisch-redaktionellen Zwecken keine Anwendung, “wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und Informationsfreiheit in

Einklang zu bringen“ (Art. 85 Abs. 2 DSGVO i. V. m. § 36 Abs. 1 rbb-Staatsvertrag i. V. m. § 19 Abs. 1, S. 1 Berliner Datenschutzgesetz bzw. §12 Abs.1 Medienstaatsvertrag/MStV). Nach dem Wortlaut dieser Vorschriften findet Art. 9 DSGVO im Zusammenhang mit journalistisch-redaktionellen Tätigkeiten keine Anwendung. Allerdings kann das Medienprivileg in seinem sachlichen Anwendungsbereich nur so weit reichen, wie die Öffnungsklausel des Art. 85 Abs. 2 DSGVO Abweichungen von ihren Vorgaben zulässt. Denn die DSGVO findet als europäische Verordnung unmittelbare Anwendung in den Mitgliedsstaaten der EU und ist in allen ihren Teilen verbindlich. Die Öffnungsklausel des Art. 85 Abs. 2 DSGVO ist angesichts der Meinungsäußerungsfreiheit weit auszulegen. Erfasst werden sämtliche Phasen der journalistischen Datenverarbeitung von der Recherche über die redaktionellen Entscheidungen, die publizistische Verwertung der Daten bis hin zur Dokumentation und Archivierung der Daten. Der Rahmen des Art. 85 Abs. 2 DSGVO ist maßgeblich durch zwei Faktoren begrenzt: zum einen durch den „journalistischen Zweck“, zum anderen durch die „Erforderlichkeit“. Bei der Beurteilung ist die von der Rechtsprechung dem öffentlich-rechtlichen Rundfunk zugesprochene Bestands- und Entwicklungsgarantie zu berücksichtigen. Danach wird der Bestand des Rundfunks auf Dauer garantiert, so dass er nicht auf seinen gegenwärtigen Entwicklungsstand beschränkt werden darf. Die Entwicklungsgarantie umfasst neben der programmlichen und finanziellen Gestaltung gerade auch die eingesetzten technischen Mittel. Wegen der dynamischen Entwicklungen im Rundfunkbereich gestattet sie es den Rundfunkanstalten, neue Formate und Technologien zu entwickeln. Dies gilt zuvorderst für die Erprobung neuer Verbreitungswege, etwa über Telemedien. Nichts anderes kann jedoch für die eingesetzten Mittel zur Produktion gelten. Auch in dieser Hinsicht darf sich der Rundfunk dem dynamischen Wandel der Technik nicht verschließen. Insofern kann die beim rbb probeweise praktizierte biometrische Datenanalyse mittels KI hier als erforderlich angesehen werden. Selbstverständlich gebietet die besondere Eingriffsintensität auch eine besondere Sorgfalt bei den TOM zur Vermeidung jeglicher missbräuchlichen Verwendung der Daten.

3. Leitlinien zum Datenschutz in den Telemedien-Angeboten von ARD, ZDF und Deutschlandradio

Eine Arbeitsgruppe aus Mitgliedern des AK DSB hat im Herbst/Winter 2021 die aus dem Jahr 2016 stammenden Leitlinien des AK DSB zum Datenschutz in den Telemedien- und Social-Media-Angeboten vollständig überarbeitet und an die aktuelle Rechtslage angepasst. Diese Anpassung war nach dem Erlass einiger wichtiger EuGH-Urteile und dem Inkrafttreten des TTDSG (s. Kap. B. II. 1.1) erforderlich geworden. Ich habe die sehr aufwändige redaktionelle Arbeit koordiniert. Im Februar 2022 hat der AK DSB die neuen „Leitlinien zum Datenschutz in den Telemedien-Angeboten von ARD, ZDF und Deutschlandradio“ verabschiedet (Anlage). Ziel ist es, sie künftig in kürzeren Abständen zu aktualisieren.

4. Neue Distributionsplattformen

Der rbb verbreitet seine Angebote zunehmend auch über Drittplattformen. Dies entspricht seinem gesetzlichen Auftrag (§§ 30 ff. MStV) und ist vor dem Hintergrund des geänderten Nutzungsverhaltens der Rezipient:innen geboten. Aus Datenschutzsicht sind viele Plattformen kritisch zu betrachten. Problematisch ist die Präsenz auf den Drittplattformen insbesondere dann, wenn von einer gemeinsamen Verantwortlichkeit für die Verarbeitung der Nutzerdaten ausgegangen werden muss.

Meine kritische Haltung zur Verbreitung des Angebots „safespace“ für Mädchen im Alter zwischen 14 und 16 Jahren mit dem Fokus auf die Themen Gesundheit und Schönheit über das Videoportal TikTok veranlasste den Programmdirektor im Jahr 2020, ein Gremium aus Mitarbeiter:innen der Online-Koordination, der Jugendschutzbeauftragten und der Datenschutzbeauftragten unter der Leitung eines Mitarbeiters der Online-Koordination zu bilden. Geplant ist, dass das Gremium in regelmäßigen Abständen zusammenkommt, um Drittplattformen als Distributionspartner für den rbb zu bewerten (s. 17. Tätigkeitsbericht, S. 53 ff.). Wir haben im Berichtzeitraum mehrfach virtuell getagt. Zunächst ging es um eine Klärung, welche Informationen die Jugendschutzbeauftragte und die Datenschutzbeauftragte benötigen, um die einzelnen Plattformen jeweils bewerten zu können. Dabei bestand für mich die Schwierigkeit darin, dass von der Rechtsprechung bislang noch nicht abschließend geklärt war, unter welchen

Voraussetzungen von einer gemeinsamen Verantwortlichkeit i. S. v. Art. 26 DSGVO des Anbieters von Inhalten und des Plattformbetreibers ausgegangen werden muss. Diese Klärung ist durch das Urteil des OVG Schleswig-Holstein am 25.11.2021 erfolgt (s. Kap. B. IV. 1.). Nun kann aus Datenschutzsicht die Arbeit des Gremiums starten. Dies habe ich dem Kollegen aus der Online-Koordination mitgeteilt.

5. Beratungstermine in den Redaktionen

Auch im Berichtszeitraum hat die Datenschutzbeauftragte wieder einzelne Bereiche der Programmdirektion zur Umsetzung datenschutzrechtlicher Anforderungen beraten. In folgenden Bereichen fanden Einzelberatungen statt:

- 21.4.2021 Produktionsleitungen
- 28.4.2021 Politische Talkformate
- 21.9.2021 Leitung Contentbox Gesellschaft

Themen waren u. a. die Verfahren bei Akkreditierungen, beim On-Boarding freier Mitarbeiter:innen, bei der Disposition von Mitarbeiter:innen und bei Auftragsverarbeitungsverhältnissen im Zusammenhang mit Produktionen. Außerdem wurden die wichtigsten Regelungen der DA Informationsmanagement vermittelt.

Am 13.7.2021 hatte ich im Rahmen eines sogenannten „Boxenstopps“ in einer Videokonferenz der Programmdirektion die Gelegenheit, wichtige Themen des Datenschutzes den leitenden Mitarbeiter:innen in der Programmdirektion zu vermitteln. U. a. bin ich auf die oftmals schwierige Abgrenzung zwischen Auftragsverarbeitung und Joint Controlling bei der Beauftragung externer Dienstleister eingegangen.

VI. Sonstiges

1. Datenschutz in der Abteilung Medienforschung

Auch im Berichtsjahr fand wieder ein reger Austausch mit der Leitung und den Mitarbeiter:innen der Abteilung Medienforschung statt. Im Fokus standen datenschutzrechtliche Fragen im Zusammenhang mit der Durchführung von Publikumsgesprächen und Interviews für Format- bzw. Programmentwicklung und der Rekrutierung der Proband:innen dafür. Während der rbb die Gespräche und Interviews in der Regel selbst durchführt, wird mit der Rekrutierung und Honorierung der Proband:innen regelmäßig eine Agentur beauftragt. Da die Agentur die Proband:innen teilweise auch für eigene Zwecke rekrutiert und in einer Datei auch für Einsätze bei anderen Kund:innen vorhält, liegt ein Fall der gemeinsamen Verantwortung (Art. 26 DSGVO – Joint Controller) für die Datenverarbeitung vor. Der rbb hat aus diesem Grund mit der Agentur einen Joint-Controller-Vertrag abgeschlossen. Danach ist die Agentur für die Korrektheit der Datenverarbeitung im Zusammenhang mit der Rekrutierung, Organisation und Honorierung der Teilnehmer:innen verantwortlich. Dem rbb obliegt die datenschutzkonforme Durchführung der Interviews. Zusammen mit mir wurden sämtliche Dokumente für die Publikumsgespräche wie Joint-Controller-Vertrag, Datenschutzerklärungen u. a. erstellt. Anschließend wurde das Verfahren in das VVT aufgenommen.

2. Datenschutz in der Abteilung Marketing und PR

Eine intensivere Zusammenarbeit fand im Berichtsjahr auch wieder mit den Kolleginnen und Kollegen aus der Abteilung Marketing und PR statt. Die Einführung und Nutzung der Corona-Warn-App und der Luca-App zur Kontaktnachverfolgung bei Veranstaltungen war in enger Abstimmung mit mir erfolgt. Zum 5.2.2022 ist die Pflicht zur Anwesenheitsdokumentation bei Veranstaltungen weggefallen. Seitdem sind beide Apps nicht mehr im Einsatz.

D. Datenschutz beim Rundfunkbeitragseinzug

I. Allgemeines

Für den Einzug der Rundfunkbeiträge betreiben die Landesrundfunkanstalten auf der Grundlage von § 10 Abs. 7 RBStV im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft den Zentralen Beitragsservice (ZBS) in Köln. In der Verwaltungsvereinbarung Rundfunkbeitragseinzug von ARD, ZDF und Deutschlandradio wird die Struktur des ZBS beschrieben und seine Aufgaben von denen der dezentralen Einheiten in den jeweiligen Landesrundfunkanstalten abgegrenzt.

Soweit der ZBS für den rbb tätig wird, gelten neben der DSGVO und den bereichsspezifischen Datenschutzregelungen des RBStV ergänzend die Regelungen des BlnDSG. Die betriebliche Datenschutzbeauftragte des rbb ist gemäß § 4 BlnDSG für die Überwachung der ordnungsgemäßen Datenverarbeitung beim Beitragseinzug zuständig. Zuständige Aufsichtsbehörde gemäß Art. 51 DSGVO ist die Beauftragte für den Datenschutz des Landes Berlin (§ 38 Abs. 8 rbb-StV).

Unbeschadet der Zuständigkeit des/der nach Landesrecht für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ist beim ZBS gemäß § 11 Abs. 2 Satz 1 RBStV ein:e behördliche:r Datenschutzbeauftragte:r zu bestellen. Die/der behördliche Datenschutzbeauftragte arbeitet zur Gewährleistung des Datenschutzes mit dem/der nach Landesrecht für die jeweilige Rundfunkanstalt zuständigen Datenschutzbeauftragten zusammen und unterrichtet diese:n über Verstöße gegen Datenschutzvorschriften sowie über die dagegen getroffenen Maßnahmen. Im Übrigen gelten die für die bzw. den behördliche:n Datenschutzbeauftragte:n anwendbaren Bestimmungen der DSGVO entsprechend. Die behördliche Datenschutzbeauftragte des rbb und ihr Stellvertreter sind Mitglieder des AK DSB. Durch die Mitgliedschaft ist ein zeitnaher Austausch zu Datenschutzfragen im Zusammenhang mit dem Beitragseinzug gewährleistet. Um komplexere Themen besser vorbereiten zu können, hat der AK DSB einen Unterarbeitskreis ‚Beitragsdatenverarbeitung' gegründet, dessen Mitglied auch die rbb-Datenschutzbeauftragte ist.

In Ergänzung zur Verwaltungsvereinbarung „Rundfunkbeitragseinzug“ i. d. F. vom 16.4./18.6.2019 (VV „Rundfunkbeitragseinzug“) haben die Rundfunkanstalten eine Joint-Controller-Vereinbarung zur gemeinsamen Verantwortlichkeit bei der Datenverarbeitung im Rahmen des Rundfunkbeitragseinzugs geschlossen. Darin ist die konkrete Aufteilung der datenschutzrechtlichen Verantwortlichkeiten geregelt. Die wesentlichen Teile der Joint-Controller-Vereinbarung vom 6.5./12.5.2020 sind auf der Webseite des ZBS veröffentlicht. Darüber hinaus wird Briefen zum Zweck der erstmaligen Kontaktaufnahme zu (potentiellen) Beitrags-Schuldner:innen eine entsprechende Information beigelegt.

II. Neuer Inkassodienstleister

Hatten die staatlichen Vollstreckungsorgane keinen Erfolg bei der Beitreibung einer Rundfunkbeitragsforderung, so haben die Rundfunkanstalten in der Vergangenheit die Fa. Creditreform Mainz damit beauftragt, die Schuldner:innen nochmals anzuschreiben, um Zahlungen zu erreichen. Seit dem 1.1.2021 ist die Paigo GmbH als Inkassodienstleister für die Rundfunkanstalten im Einsatz. Der Wechsel des Inkassodienstleisters ist in datenschutzrechtlicher Hinsicht durch die Datenschutzbeauftragte des ZBS mit Unterstützung des Datenschutzbeauftragten des SWR intensiv begleitet worden. Da das Unternehmen im Auftrag der Rundfunkanstalten tätig wird, wurde ein neuer Auftragsverarbeitungsvertrag abgeschlossen sowie ein umfangreiches, 52-seitiges „Verfahrenshandbuch über die Inkassodienstleistungen“ verfasst. Seitens der von der Paigo GmbH angeschriebenen Personen kam es im Berichtszeitraum zu vermehrten Nachfragen zum Rechtsverhältnis zwischen der Paigo GmbH und den Rundfunkanstalten. Hierzu hat die Paigo GmbH in Abstimmung mit dem ZBS ein Schreiben entwickelt, das dieses Rechtsverhältnis in datenschutzrechtlicher Hinsicht näher erläutert.

III. Löschung von nicht mehr benötigten Beitragsschuldnerdaten

Das Projekt zur Umsetzung des neuen Löschkonzepts (s. 17. Tätigkeitsbericht, S. 61) konnte im Berichtsjahr erfolgreich abgeschlossen werden. Für die langfristige Aufrechterhaltung der DSGVO-Konformität wurden neue „Housekeepings“ erstellt und/oder existierende

„Housekeepings“ angepasst sowie entsprechende Dokumentationen erstellt. (Unter „Housekeeping“ versteht man routinemäßige Tätigkeiten, deren Ziel es ist, die Funktion und Leistungsfähigkeit eines IT-Systems zu erhalten.) Die bis dahin im Projekt EUDAGO PRO liegenden Verantwortlichkeiten wurden auf die zuständigen Fachbereiche des ZBS übertragen.

IV. Auskunftsersuchen und Eingaben

1. Bearbeitung von Auskunftsersuchen und Eingaben durch den ZBS

Die Rundfunkanstalten haben die Bearbeitung von datenschutzrechtlichen Anfragen und sonstigem Routineschriftwechsel in Beitragsangelegenheiten dem ZBS übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter und von individuellen Anfragen mit besonderer datenschutzrechtlicher Bedeutung haben sie sich selbst vorbehalten.

Wie berichtet, ist der Auskunftsanspruch in Bezug auf die Beitragsschuldnerdaten in § 11 Abs. 8 RBStV mit Wirkung zum 1.6.2020 neu geregelt worden (s. 17. Tätigkeitsbericht, S. 61). Wesentliche Änderung ist, dass Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, vom datenschutzrechtlichen Auskunftsanspruch nicht umfasst sind. Übergangsweise wurde in denjenigen Fällen, in denen zunächst der alte Auskunftsbrief versandt worden war, noch auf Wunsch die erweiterte Auskunft versandt. Zum 8.9.2021 erfolgte die endgültige Einstellung des Versands der erweiterten Stufe. Neben der Möglichkeit, ein schriftliches Auskunftsersuchen an den ZBS zu richten, besteht die Möglichkeit, eine Datenschutzauskunft elektronisch zu beantragen. Für den Abruf über das ZBS-Onlineportal werden in diesem Fall vorab vom ZBS die Zugangsdaten per Post an die Auskunftsuchenden versandt.

Im Zeitraum 1.1.bis 31.12.2021 hat der ZBS für den rbb insgesamt 626 (Vorjahr 2.787) einfache Datenauskünfte erteilt, davon 259 auf elektronischem Weg über das Onlineportal. Eine erweiterte Datenauskunft wurde nur in zwei Fällen beantragt und antragsgemäß erteilt.

Die nachfolgende Übersicht liefert einen Überblick über die monatliche Entwicklung der datenschutzrechtlichen Eingaben bzw. der entsprechend ausgelösten Briefe beim ZBS für alle Landesrundfunkanstalten im Jahr 2021 zusammengefasst:

Jan.	**Feb.**	**März**	**April**	**Mai**	**Juni**	**Juli**	**Aug.**	**Sep.**	**Okt.**	**Nov.**	**Dez.**
915 (396)	785 (317)	701 (265)	577 (270)	560 (258)	471 (186)	389 (97)	493 (131)	420 (197)	519 (273)	452 (230)	606 (235)

(Bei den in Klammern angegebenen Werten handelt es sich um die elektronisch beantragten einfachen Datenauskünfte.)

2. Bearbeitung von Auskunftsersuchen und Eingaben durch die Datenschutzbeauftragte des rbb

Bei der Datenschutzbeauftragten des rbb sind zur Beitragsdatenverarbeitung im Zeitraum 1.1.bis 31.12.2021 insgesamt ein Auskunftsersuchen und eine Rückfrage zu einer durch den ZBS erteilten Auskunft eingegangen. (Zum Vergleich: Im Jahr 2020 waren es noch insgesamt 13 Auskunftsersuchen und Eingaben zur Beitragsdatenverarbeitung). Das Auskunftsersuchen habe ich – wie im Joint-Controller-Vertrag festgelegt – direkt an den ZBS zur Bearbeitung abgegeben. Mit der Rückfrage erkundigte sich der Petent nach der Rechtsgrundlage für die Speicherung der aktuell und früher genutzten Bankverbindungen für erhaltene Überweisungen beim ZBS. Ich habe ihm als Rechtsgrundlage für die Aufbewahrung der Bankverbindungsdaten § 257 Abs. 4 i. V. m. § 257 Abs. 1 Nr. 1 und 4 Handelsgesetzbuch (HGB) genannt.

V. Beschwerden zur Datenverarbeitung beim Beitragseinzug

Über die zuständige Aufsichtsbehörde, die Berliner Beauftragte für Datenschutz (BlnDSB), erreichten die rbb-Datenschutzbeauftragte insgesamt fünf Beschwerden.

In einer Beschwerde wurde der Inhalt der durch den ZBS erteilten Auskunft gerügt. Zum einen wurde angezweifelt, dass die handels- und steuerrechtlichen Aufbewahrungspflichten auf die Datenverarbeitung im Beitragswesen Anwendung finden. Außerdem rügte der

Beschwerdeführer, dass die ihm erteilte Auskunft unvollständig sei. Die Aufsichtsbehörde wies in diesem Zusammenhang darauf hin, dass nach ihrer Auffassung die durch den 23. Rundfunkänderungsstaatsvertrag in Bezug auf Art. 15 DSGVO vorgenommene Beschränkung des Auskunftsrechts (§ 11 Abs. 8 RBStV) gegen europarechtliche Vorgaben verstoße. Sie prüfe derzeit, welche Konsequenzen daraus für das aufsichtsbehördliche Handeln zu ziehen sind. Ich habe daraufhin der Aufsichtsbehörde die Beachtlichkeit der Aufbewahrungsfristen nach HGB und Abgabenordnung näher erläutert. Außerdem habe ich darauf hingewiesen, dass der Beschwerdeführer im Jahr 2020 noch im zweistufigen Verfahren eine Datenauskunft erhalten hatte und somit der neue § 11 Abs. 8 RBStV, der eine eingeschränkte Auskunftserteilung regelt, in diesem Fall gar keine Rolle gespielt hat. Außerdem habe ich der Behörde wunschgemäß das aktualisierte Löschkonzept des ZBS zugesandt.

Eine andere Beschwerde richtete sich gegen die Anforderung umfangreicher Unterlagen durch den ZBS im Zusammenhang mit einem Antrag auf Härtefall-Befreiung von der Rundfunkbeitragspflicht. In meiner Stellungnahme gegenüber der Aufsichtsbehörde habe ich die Notwendigkeit der einzelnen Dokumente für die Härtefall-Prüfung dargelegt und die entsprechenden Rechtsgrundlagen genannt.

Eine weitere Beschwerde richtete sich dagegen, dass ein an den Beschwerdeführer gerichtetes Schreiben vom ZBS nicht an seine Postadresse, sondern an die Adresse seiner Eltern gerichtet war. Nach Rücksprache mit dem ZBS konnte ich der Aufsichtsbehörde mitteilen, dass der ZBS die vermeintliche Adresse der Eltern (darüber, ob dies tatsächlich der Fall ist, hat der ZBS keine Kenntnis) im Rahmen eines Nachsendeverfahrens der Deutschen Post erhalten hatte. Nach der Postdienste-Datenschutzverordnung darf die Post einem Dritten auf sein Verlangen hin Auskunft darüber erteilen, ob die angegebene Anschrift eines am Postverkehr Beteiligten richtig ist, soweit es für Zwecke des Postverkehrs erforderlich ist. In § 40 Postgesetz ist geregelt, dass die Post Gerichten und Behörden auf deren Verlangen die zustellfähige Anschrift eines am Postverkehr Beteiligten mitteilt, soweit dies für Zwecke des Postverkehrs der Gerichte oder Behörden erforderlich ist. Dies gilt auch dann, wenn der Empfänger eine für die Übermittlung erforderliche Einwilligung nicht erteilt, oder gegen die Übermittlung Widerspruch erhoben hat. Der ZBS ist „Behörde“ im Sinne des § 40 Postgesetz.

Die vierte Beschwerde betraf eine nicht innerhalb der gesetzlich vorgeschriebenen Monatsfrist erteilte Auskunft durch den ZBS. Nach Rücksprache mit den Kollegen beim ZBS konnte ich der Aufsichtsbehörde die Verkettung von Fehlverhalten zweier beteiligter Sachbearbeiter erläutern, die dazu geführt hatte, dass das Auskunftsersuchen zunächst nicht als solches erkannt und zur normalen Post gegeben, weshalb es nicht mit der für die Auskunftsersuchen festgelegten Priorität bearbeitet worden war. Außerdem habe ich der Aufsichtsbehörde die Abhilfemaßnahmen beschrieben, die der ZBS zur Vermeidung vergleichbarer Fehlverhalten in der Zukunft ergriffen hat. (In drei älteren Fällen, mit denen der rbb schon im vorhergehenden Berichtszeitraum konfrontiert war und in denen die Auskunftsersuchen jeweils nicht fristgerecht durch den ZBS beantwortet worden waren, hat die Aufsichtsbehörde jeweils eine förmliche Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO gegenüber dem rbb ausgesprochen – dies, obwohl ich in allen drei Fällen nach Rücksprache mit dem ZBS gegenüber der Behörde ausgeführt hatte, dass der ZBS inzwischen umfangreiche TOM ergriffen hat, um derartige Verzögerungen zukünftig zu vermeiden.)

In dem fünften Verfahren hatte der Beschwerdeführer vom ZBS ein Schreiben erhalten, in dem ihm mitgeteilt wurde, er habe sein Beitragskonto auf eine andere Person umschreiben wollen. Er gab an, einen solchen Antrag nie beim ZBS gestellt zu haben. Seine Nachfrage beim ZBS sei zunächst unbeantwortet geblieben. Der Sachverhalt wurde dem Beschwerdeführer und der Aufsichtsbehörde nach Rücksprache mit dem ZBS erläutert. Eine unbefugte Person hatte versucht, per Internet-Formularanmeldung unter der Teilnehmernummer des Beschwerdeführers eine Kontenänderung herbeizuführen. Dies konnte durch das Schreiben an den Beschwerdeführer aufgeklärt werden. Aus Datenschutzgründen konnte dem Beschwerdeführer der Name der unbefugten Person nicht mitgeteilt werden.

E. Informationsverarbeitungszentrum

I. Allgemeines

Das Informationsverarbeitungszentrum (IVZ) ist eine Kooperation aller Landesrundfunkanstalten sowie von Deutschlandradio und Deutscher Welle in Form einer öffentlich-rechtlichen nichtrechtsfähigen Verwaltungsgemeinschaft. Das IVZ ist beim rbb angesiedelt und auch an den Standorten anderer Landesrundfunkanstalten aktiv. Die Landesrundfunkanstalten kooperieren über das IVZ rund um die SAP-Anwendungen sowie bezüglich der Archiv- und Produktionssysteme.

II. Joint-Controller-Vertrag

Die inhaltliche und rechtliche Grundlage der IVZ-Kooperation bildet die IVZ-Verwaltungsvereinbarung. In Ergänzung dazu haben die Intendantinnen und Intendanten am 22.9.2020 eine Vereinbarung zur gemeinsamen Verantwortlichkeit bei der Verarbeitung von personenbezogenen Daten beim IVZ (Joint-Controller-Vertrag gemäß Art. 26 DSGVO) abgeschlossen. Darin sind u. a. die Zwecke und Mittel der Datenverarbeitung, die Erfüllung der datenschutzrechtlichen Verpflichtungen, die TOM zur Datensicherheit und die Informationspflichten des IVZ geregelt. Für die Kontrolle des Datenschutzes sind alle Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Als Datenschutzbeauftragte der Sitzanstalt ist die Datenschutzbeauftragte des rbb federführend für das IVZ zuständig. Zusätzlich hat das IVZ laut Joint-Controller-Vertrag einen eigenen Datenschutzbeauftragten zu bestellen, der die anfallenden Aufgaben nach Art. 39 DSGVO wahrnimmt. Der betriebliche Datenschutzbeauftragte des IVZ arbeitet mit den Datenschutzbeauftragten der für die jeweilige Datenverarbeitung zuständigen Rundfunkanstalten kooperativ zusammen. Er erstellt einen jährlichen Tätigkeitsbericht.

III. Umgang mit den IT-Restrisiken

Die im IVZ angewendete ISO 27001 ist eine risikobasierte IT-Sicherheitsnorm. Dabei wird der zu zertifizierende IT-Verbund entsprechend den Vorgaben der Norm in einer Anwendbarkeitserklärung dargestellt. Danach wird das Risikomanagementkonzept auf den zu zertifizierenden IT-Verbund angewendet. Das IVZ ist laut Verwaltungsvereinbarung dazu verpflichtet, sich an den Vorgaben des BSI zu orientieren. Daher werden die 47 elementaren Grundschutzbedrohungen als mögliche Risiken angenommen. Alle Anwendungsbereiche des IVZ werden für alle Grundschutzbedrohungen hinsichtlich Eintrittswahrscheinlichkeit und Auswirkung bewertet. Laufend werden für die einzelnen Geschäftsprozesse Risikoanalysen erstellt. Durch Maßnahmen werden die erkannten Risiken so weit gesenkt, dass keine hohen Risiken verbleiben. Mittlere Risiken werden dem IVZ-Lenkungsausschuss zur Bestätigung in einem Quartalsbericht vorgelegt. Am 26.8.2021 nahmen Mitglieder des AK DSB und die Informationssicherheitsbeauftragten der am IVZ beteiligten Häuser an der IVZ-Lenkungsauschuss-Sitzung zur Liste der Restrisiken als beratende Gäste teil. Da diese Liste den Mitgliedern des AK DSB erst kurzfristig vor der Sitzung zur Verfügung gestellt worden war, wurde verabredet, diese in einer Sondersitzung des AK DSB zu behandeln. Dies ist am 7.10.2021 geschehen. Nach eingehender Behandlung wurde die Liste der Restrisiken im AK DSB zur Kenntnis genommen und bestätigt. Die Datenschutzbeauftragten haben darum gebeten, dass die neuen Risiken der Liste zukünftig jeweils mit einem Votum des betrieblichen Datenschutzbeauftragten versehen werden, um auszuschließen, dass rein betriebswirtschaftliche Kriterien bei der Entscheidung über die Akzeptanz der Restrisiken eine Rolle spielen. Die Quartalsberichte werden jeweils vor Behandlung im Lenkungsausschuss mit der rbb-Datenschutzbeauftragten besprochen. Sie entscheidet im jeweiligen Einzelfall, ob zusätzlich eine Befassung des gesamten AK DSB mit den neuen Restrisiken erforderlich ist.

Am 29.11.2021 fand ein erstes Quartalsgespräch statt, an dem neben dem betrieblichen Datenschutzbeauftragten auch der Informationssicherheitsbeauftragte des IVZ und dessen Stellvertreter teilnahmen. Ein weiteres Quartalsgespräch fand am 28.3.2022 statt.

IV. IVZ-Jahrestreffen

Einmal jährlich findet beim IVZ das ‚Jahrestreffen IT-Sicherheit und Datenschutz' statt. Auf diesem Treffen informiert der Geschäftsführer u. a. über datenschutzrelevante Themen des zurückliegenden Jahres. Das letzte Jahrestreffen fand am 2.12.2021 per Videokonferenz statt. Einen Schwerpunkt bildete der Entwurf des ersten Datenschutzberichts des betrieblichen Datenschutzbeauftragten des IVZ und das Ergebnis einer von ihm durchgeführten DSFA für den Einsatz von Microsoft 365 im IVZ. Die Diskussion zeigte, dass es u. a. noch Unklarheiten bezogen auf die Kontrollzuständigkeiten der für das IVZ zuständigen Aufsichtsbehörden und die im Joint-Controller-Vertrag festgelegten Aufgaben des IVZ wie Bearbeitung von Auskunftsersuchen, Prüfung von Auftragsverarbeitern etc. und dem Umgang mit Sicherheitsvorfällen gibt. Eine Intensivierung des Informationsaustauschs zwischen den IVZ-Verantwortlichen und der rbb-Datenschutzbeauftragten wurde vereinbart.

F. ARD-Generalsekretariat

I. Allgemeines

Das ARD-Generalsekretariat (ARD-GS) unterstützt den üblicherweise alle zwei Jahre wechselnden Vorsitz der ARD bei der Geschäftsführung des Senderverbunds und der strategischen Positionierung der ARD, der Interessenvertretung nach außen und der Öffentlichkeitsarbeit. Wie alle anderen GSEA der ARD unterliegt auch das ARD-GS der gemeinsamen Aufsicht der Datenschutzbeauftragten der Landesrundfunkanstalten und der Deutschen Welle. Nach dem Federführungsprinzip ist die rbb-Datenschutzbeauftragte für die Beratung und Kontrolle vor Ort zuständig.

II. Joint-Controller-Vertrag

Der vor diesem Hintergrund notwendige Joint-Controller-Vertrag zwischen dem ARD-GS und den beteiligten Rundfunkanstalten wurde von deren Justitiariaten in Abstimmung mit dem AK DSB entworfen und befindet sich derzeit noch in der Abstimmung.

III. Neues Dokumentenmanagement-System

Für das ARD-GS gehört es zur täglichen Arbeit, Informationen aus allen Bereichen der ARD zu sammeln, zu strukturieren und für unterschiedliche Anlässe und Termine aufzubereiten. Dabei entstehen zum einen aktuelle Dokumente wie E-Mail-Korrespondenzen und Sitzungsvorlagen. Daneben existiert aber auch ein umfangreiches digitalisiertes Schriftgutarchiv, das bis in die 1960er Jahre zurückreicht, derzeit ca. 450.000 Dokumente umfasst und jährlich um ca. 4.500 Dokumente anwächst. Die technische Basis für das Schriftgutarchiv bildete bislang das Presse-Archiv-Netzwerk (PAN). Da dessen Abschaltung für das erste Quartal 2022 anstand, musste hierfür eine Ersatzlösung gefunden werden. Außerdem sollte das Auffinden, Zusammenstellen und arbeitsteilige Weiterverarbeiten unterschiedlicher Materialien vereinfacht werden. Daher hat sich das ARD-GS dafür entschieden, zukünftig mit dem Dokumentenmanagement-System (DMS) „Shareflex“ zu arbeiten. Dabei handelt es sich um eine cloudbasierte Lösung auf der Basis von Microsoft 365. In die Planungen wurde ich von Anfang an einbezogen (s. 17. Tätigkeitsbericht, S. 66). Auf der Sitzung des AK DSB am 22.4.2021 habe ich über das Projekt berichtet. Der AK DSB hat das Projekt positiv bewertet. Die für die Aufnahme in das VVT erforderlichen Dokumente hat mir das ARD-GS im Laufe des vergangenen Jahres nach und nach vorgelegt. Danach konnte ich dem für den Zeitraum 3.1. bis 30.6.2022 geplanten Probebetrieb zustimmen und das Verfahren in das VVT aufnehmen. Die Vertraulichkeit der Dokumente ist durch eine Verschlüsselung in der Anwendung „SharePoint“ seitens Microsoft gewährleistet. Streng vertrauliche Daten legt das ARD-GS nicht in dem Dokumentensystem ab. Eine spezielle Backup-Lösung wird noch entwickelt. Der historische Datenbestand wurde auf einer externen Festplatte gespiegelt, die im ARD-GS eingeschlossen ist. Auf dieser Grundlage könnte eine erneute Migration des Bestandes bis einschließlich 2021 erfolgen.

G. ARD-Hauptstadtstudio

I. Allgemeines

Rund 70 Korrespondentinnen und Korrespondenten aus allen Landesrundfunkanstalten beliefern täglich die Redaktionen der ARD in Fernsehen, Hörfunk und Online mit Nachrichten, Interviews, Hintergrundinformationen und Kommentaren zu bundespolitischen Themen aus dem ARD-Hauptstadtstudio (ARD-HSB).

Für die datenschutzrechtliche Aufsicht über das ARD-HSB sind – wie bei allen GSEA – die Datenschutzbeauftragten der beteiligten Rundfunkanstalten gemeinsam zuständig. Federführend betreut die rbb-Datenschutzbeauftragte das ARD-HSB.

II. Joint-Controller-Vertrag

Der für das ARD-HSB notwendige Joint-Controller-Vertrag wurde von den Justitiariaten der beteiligten Rundfunkanstalten in Abstimmung mit dem AK DSB entworfen und befindet sich derzeit in der Abstimmung.

III. Austausch zu datenschutzrechtlichen Themen mit dem Leitungsteam

Im Berichtsjahr hatte ich mich an die Leiterin des ARD-HSB Frau Tina Hassel gewandt und um Benennung eines Datenschutz-Koordinators bzw. einer Datenschutz-Koordinatorin gebeten, um den Informationsfluss zwischen dem HSB und der rbb-Datenschutzbeauftragten zu intensivieren. Daraufhin lud mich Frau Hassel in das ARD-HSB ein, um mein Anliegen näher zu erläutern und die Hintergründe darzustellen. Auf meinen Vorschlag hin wurden Gegenstand und Teilnehmerkreis des Treffens erweitert. Gemeinsam mit dem rbb-Informationssicherheitsbeauftragten habe ich am 1.11.2021 dem gesamten Leitungsteam des ARD-HSB einen Überblick über die Grundprinzipien des Datenschutzes und der Informationssicherheit gegeben und das Datenschutzmanagementsystem für den rbb einschließlich der GSEA unter seiner

Federführung vorgestellt. Im Nachgang benannte Frau Hassel die Verwaltungsleiterin des ARD-HSB, Frau Simone Lenzen, zur Datenschutz-Koordinatorin für das ARD-HSB.

H. Sonstige Auskunftsersuchen, Eingaben und Beschwerden

Neben den unter Kapitel D. IV. 2. erwähnten Auskunftsersuchen zur Beitragsdatenverarbeitung haben die rbb-Datenschutzbeauftragte im Jahr 2021 außerdem sechs unspezifische Auskunftsersuchen und drei unspezifische Löschbegehren erreicht. Auf diese Anträge habe ich zunächst mit einem standardisierten Zwischenbescheid reagiert und um eine Konkretisierung der Begehren gebeten. Ziel dieses zweistufigen Verfahrens ist es, eine gezielte und datensparsame Abfrage innerhalb des rbb zu ermöglichen. Auf meine Zwischenbescheide wurde lediglich in insgesamt fünf Fällen nochmals reagiert: Vier Auskunftsersuchen und ein Löschbegehren wurden danach ausdrücklich auf sämtliche Bereiche des rbb bezogen. In zwei Fällen konnte eine Datenverarbeitung im Bereich Beitragsservice und Justitiariat festgestellt und dies den Petenten mitgeteilt werden. Von einem Antragsteller waren personenbezogene Daten im System der Service-Redaktion vorhanden, da er sich zu einem Programmangebot des rbb geäußert hatte und die Aufbewahrungsfrist noch nicht abgelaufen war. In einem Fall konnte der Antragstellerin mitgeteilt werden, dass zu ihrer Person keine Daten innerhalb des rbb vorhanden waren. Auch das Löschbegehren ging ins Leere, weil keine personenbezogenen Daten des Antragstellers im rbb vorhanden waren.

Insgesamt elf sonstige Eingaben und Beschwerden sind bei der rbb-Datenschutzbeauftragten im Jahr 2021 eingegangen.

Aus dem Kreis der Kolleginnen und Kollegen erreichte mich eine Beschwerde zu den Speicherfristen im Dienstplan-Tool „Team-Plan“. Es stellte sich heraus, dass die Beschwerde auf einer Fehlinterpretation der Datenschutzerklärung für „Team-Plan“ beruhte. Es ging um die Speicherfristen, die der Fachbereich gemeinsam mit mir festgelegt hatte. Eine anonyme Beschwerde bezog sich auf eine Anwendung innerhalb der Dispositionssoftware MIRAAN. Die

Beschwerde wurde zur Kenntnis genommen und ihr Inhalt bei der datenschutzrechtlichen Begleitung der finalen Konfiguration von MIRAAN berücksichtig (s. Kap. C. IV. 7.).

Ein Beschwerdeführer kritisierte, dass er auf sein gleichlautendes Schreiben an alle Intendant:innen in einer rundfunkpolitischen Angelegenheit eine Antwort vom ZBS erhalten hatte. Diese im Auftrag der Intendant:innen erteilte Antwort des ZBS war als E-Mail ohne Ende-zu-Ende-Verschlüsselung an ihn versandt worden. Ich teilte dem Beschwerdeführer mit, dass eine Transportverschlüsselung in diesem Fall ausreichend war, da der Inhalt der Mail keinen erhöhten Schutzbedarf aufwies.

Wie auch meine Kolleg:innen der anderen Rundfunkanstalten erreichten mich kritische Anmerkungen einer Person per E-Mail zur Präsenz des öffentlich-rechtlichen Rundfunks auf Social Media, zur Verbreitung seiner Angebote über Sprachassistenten und zur Kommunikation mit seinen Rezipient:innen per Messenger-Diensten. Nach Einschätzung der Absenderin konnten Passagen der rbb-Datenschutzerklärung als Anreiz verstanden werden, die aufgelisteten Social-Media-Plattformen etc. zu nutzen. Außerdem vermisste sie eine Aktivität auf dem vom Bundesdatenschutzbeauftragten empfohlenen Social-Media-Kanal „Mastodon“. Ich habe die Absenderin auf die Tatsache hingewiesen, dass die Bedeutung der klassischen Programmverbreitungswege zu Lasten von Drittplattformen/Intermediären immer weiter abnimmt. Um insbesondere auch das junge Publikum weiterhin zu erreichen und um neue Zielgruppen zu erschließen, verbreitet der rbb seine Programminhalte auch über Plattformen Dritter. Dies entspricht seinem gesetzlichen Programmauftrag (§§ 30 ff. MStV). Dabei findet kontinuierlich eine datenschutzrechtliche Prüfung der Plattformen statt, da sich diese dynamisch entwickeln. Ähnliches gilt für die Messenger-Dienste, die der rbb u. a. als Rückkanal für seine Rezipient:innen nutzt. Hierbei wird darauf geachtet, dass bei Gewinnspielen u. ä. neben WhatsApp und Co. immer auch eine datenschutzrechtlich unkritische Alternative angeboten wird. Die Anmerkungen der Beschwerdeführerin zum Inhalt der Datenschutzerklärung habe ich zum Anlass genommen, einige kleinere Änderungen daran zu veranlassen. „Mastodon“ wurde von den Expert:innen in der rbb-Online-Koordination geprüft. Es handelt sich um einen Open-Source-Microblogging-Dienst, der als dezentrales Netzwerk von unterschiedlichen Betreibern unkommerziell betrieben wird. Das Netzwerk ist in verschiedene Gemeinschaften aufgeteilt, die miteinander verknüpft sind. Weder im Bereich Regionales noch im Bereich

Journalismus, Musik u. a. konnten bislang relevante Plattformteilnehmer, z. B. andere Medienunternehmen, festgestellt werden. Der rbb ist demgegenüber auf Plattformen vertreten, wenn dort relevante Zielgruppen und eine gewisse Reichweite für seine Angebote zu erwarten sind. Da dies bei „Mastodon“ aktuell nicht gegeben ist, wäre der Aufwand für die Drittplattformbetreuung nicht gerechtfertigt.

Eine weitere Beschwerde bezog sich auf die Verarbeitung von Nutzerdaten durch das in den Programmen des rbb genutzte Voting-Tool „meinrbb.de“. Ich musste feststellen, dass der Wortlaut der Datenschutzerklärung für dieses Tool eines US-Anbieters von der mit mir ursprünglich vereinbarten Fassung signifikant abwich. Der Hintergrund dieser Abweichung war nicht mehr aufzuklären. Ich habe die Beschwerde zum Anlass genommen, die Datenverarbeitung beim Einsatz dieses Tools erneut einer gründlichen Prüfung zu unterziehen. In diesem Zusammenhang mussten Anpassungen am Verfahren vorgenommen und die Datenschutzerklärung vollständig überarbeitet werden. Außerdem habe ich den Abschluss der neuen Standardvertragsklauseln (s. Kap. B. I. 3.) mit dem Anbieter veranlasst.

Im Vorfeld der Ausstrahlung einer rbb-Produktion hatte sich eine Person beim rbb gemeldet und Zweifel an der Objektivität des Autors geäußert. Im Nachgang beschwerte sich diese Person bei der Intendantin darüber und äußerte, dass es hinreichende Anhaltspunkte dafür gebe, dass Mitarbeitende des rbb ihre Informationen und ihren Namen unbefugt an Dritte weitergegeben hätten. Als Beleg für diesen vermeintlichen Verstoß gegen Datenschutzrecht fügte der Beschwerdeführer einen Screenshot bei, der angeblich von der Facebook-Seite des Autors des journalistischen Beitrags stammte. Die Intendantin hat die Beschwerde zuständigkeitshalber an mich zur Bearbeitung abgegeben. Nach Prüfung der Sach- und Rechtslage teilte ich dem Beschwerdeführer mit, dass ein Verstoß gegen das Datenschutzrecht nicht vorliege. Selbstverständlich hatten die Programmverantwortlichen im rbb zur Erfüllung ihrer journalistischen Sorgfaltspflichten den Autor aufgefordert, zu den vom Beschwerdeführer gelieferten Informationen Stellung zu nehmen. Dabei hatten sie aber weder den Namen des Beschwerdeführers genannt, noch seine an den rbb adressierte E-Mail an den Autor weitergeleitet.

Drei Beschwerdeführer haben sich gegen eine zeitlich befristete Sperrung der Kommentarfunktion zu Online-Angeboten des rbb gewandt. Ich habe den Beschwerdeführern jeweils

mitgeteilt, dass die Sperrung durch einen Verstoß gegen die sogenannte Netiquette begründet war. Ein Beschwerdeführer monierte eine mangelnde Überprüfung der Identität von Kommentatoren auf rbb24. Nach Rücksprache mit der Redaktion habe ich dem Beschwerdeführer geantwortet, dass auf rbb24 ohne Anmeldung anonym kommentiert werden könne. Namensgleichheiten und auch der Missbrauch von Namen ließen sich daher nicht vollständig ausschließen. Eine Beschwerdeführerin kritisierte irrtümlich den Einsatz von sogenannten Evercookies durch den rbb. Ihr konnte mitgeteilt werden, dass der rbb keine Evercookies auf seinen Online-Angeboten einsetzt.

I. Informationsmaßnahmen

Neben den in diesem Bericht an anderen Stellen bereits erwähnten spezifischen Informationsmaßnahmen habe ich im Berichtszeitraum folgende Datenschutzschulungen durchgeführt:

Gemeinsam mit dem Informationssicherheitsbeauftragten habe ich am 4.11.2021 eine Führungskräfteschulung zu den Themen Datenschutz und Informationssicherheit durchgeführt. Am 22.9.2021 habe ich zusammen mit dem stellvertretenden Informationssicherheitsbeauftragten die jährliche Datenschutzschulung für neue Auszubildende durchgeführt.

Wie berichtet, hat die HA Personal im Sommer 2019 die electronic media school (ems) damit beauftragt, ein E-Learning-Angebot zum Datenschutz im rbb zu erstellen (s. 17. Tätigkeitsbericht, S. 72 f.). Als Arbeitsgrundlage hatte die Datenschutzbeauftragte der ems ihr eigenes umfangreiches Schulungsmaterial zur Verfügung gestellt und ergänzende mündliche Erläuterungen gegeben. Im Frühjahr 2021 hat die ems die technische Umsetzung des E-Learnings fertiggestellt. Nachdem einige Änderungen vorgenommen waren, konnte das E-Learning im August 2021 auf der elektronischen Lernplattform des rbb, dem „rbb-Campus“ online gehen. Neu eingestellte Mitarbeiterinnen und Mitarbeiter erhalten seitdem automatisch im Onboarding-Prozess eine Aufforderung zur Teilnahme an der Schulung. Mittels einer Intranet-Meldung wurden alle festangestellten Mitarbeiterinnen und Mitarbeiter gebeten, die Schulung zu durchlaufen. Leider war die Teilnahme zu Anfang sehr gering. Daraufhin hat die HA Personal

das IVZ damit beauftragt, automatisierte Erinnerungs-E-Mails mit der Bitte um Teilnahme an dieser Pflicht-Schulung zu programmieren. Alle festangestellten Kolleginnen und Kollegen, die bisher noch keine Datenschutzschulung absolviert haben oder deren letzte Schulung vor dem Sommer 2018 stattfand, erhalten seit Februar 2022 solch eine automatisierte Erinnerungs-E-Mail. Die Teilnahme an der Schulung ist durch die Erinnerungen enorm gestiegen. Ziel ist, dass alle festangestellten Mitarbeiterinnen und Mitarbeiter die Schulung bis zum Sommer 2022 durchlaufen haben werden. Im nächsten Schritt ist geplant, auch die arbeitnehmerähnlich Beschäftigten durch entsprechende E-Mails zur Teilnahme aufzufordern.

J. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio

Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten arbeiten im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) zusammen. Ein wesentliches Ziel des AK DSB ist es, den Datenschutz bei den gemeinsamen Programmangeboten und beim Beitragseinzug nach möglichst einheitlichen Kriterien und Standards sicherzustellen. Zudem setzen die bei Beschaffungen immer häufiger durchgeführten Leadbuyer-Verfahren, bei dem eine Rundfunkanstalt federführend Verhandlungen auch für alle anderen Rundfunkanstalten führt, voraus, dass alle Rundfunkanstalten die gleichen Datenschutzstandards haben.

Im Berichtszeitraum fanden unter dem Vorsitz des Datenschutzbeauftragten des NDR, Herrn Dr. Heiko Neuhoff, am 22./23.4., 10.6., 12.8.,7.10. und 25./26.11.2021 Videokonferenzen des AK DSB statt.

Einen Schwerpunkt der Videokonferenz am 22./23.4.2021 bildete, wie schon in einigen zurückliegenden Konferenzen des AK DSB, das ARD-Gemeinschaftsprojekt „(D)ein SAP“ und Fragen im Zusammenhang mit geplanten Migrationstests. Außerdem wurden das Zentrale SIEM/SOC und eine geplante DSFA beim BR für Microsoft 365 behandelt.

Ein weiteres Thema war die gemeinsame Festlegung von sogenannten Informationsklassen für Daten im gesamten öffentlich-rechtlichen Rundfunk. Ein erster Anlauf von AK DSB und CC ISec (Zusammenschluss der Informationssicherheitsbeauftragten der öffentlich-rechtlichen Rundfunkanstalten), an dem ich mitgewirkt habe, ist an einem Votum der Juristischen Kommission (JuKo) gescheitert. Die JuKo bat zunächst zu klären, welche Maßnahmen mit den einzelnen Informationsklassen verknüpft sein würden. Die interdisziplinäre Arbeitsgruppe hat das ursprüngliche Dokument daraufhin überarbeitet und um technikneutrale Maßnahmen für die Informationsklassen ergänzt. Eine erneute Befassung der zuständigen Gremien in den Rundfunkanstalten steht noch aus.

In ihrer Videokonferenz vom 10.6.2021 haben sich die Mitglieder des AK DSB ausgiebig mit dem Entwurf einer Geschäftsordnung befasst. Bis dahin existierte keine Geschäftsordnung für den AK DSB. Auslöser für diese Initiative waren u. a. Abgrenzungsfragen im Zusammenhang mit einer neu gegründeten Arbeitsgruppe „Datenschutz“ innerhalb der JuKo. Der AK DSB hat bekräftigt, dass das operative Geschäft in der Zuständigkeit des Verantwortlichen (der Rundfunkanstalt) liegt und nicht den Datenschutzbeauftragten obliegt. Folgerichtig hat die JuKo im Berichtszeitraum weitere Joint-Controller-Verträge für GSEA entworfen. Unmittelbar nach Wirksamwerden der DSGVO im Jahr 2018 hatte der AK DSB für die großen GSEA ZBS, IVZ und ARD-Sternpunkte diese noch selbst erarbeitet.

Am 12.8.2021 standen unter anderem die neuen Standardvertragsklauseln, die Personalisierung der Mediatheken, ein neues Online-Nutzungsmessverfahren und Fragen im Zusammenhang mit der Abgrenzung von Auftragsverarbeitung und Joint-Controller-Verhältnissen auf der Agenda. Die Befassung mit diesen Themen wurde in der Videokonferenz vom 7.10.2021 fortgesetzt. Zu Gast waren Vertreter von ARD-Online, die uns die Funktionsweise der ARD-Mediatheken präsentiert haben. Außerdem haben wir uns mit Mindeststandards zur Authentifizierung zur Nutzung von IT-Systemen und der Präsenz der Rundfunkanstalten auf verschiedenen Drittplattformen beschäftigt.

In der Videokonferenz vom 25./26.11.2021 haben wir uns mit den Datenschutzbeauftragten der SRG (Schweizerische Radio- und Fernsehgesellschaft) ausgetauscht und sie als neue Mitglieder im AK DSB aufgenommen. Schon seit vielen Jahren ist der Datenschutzbeauftragte des

ORF Mitglied des AK DSB. Durch die Mitgliedschaft des österreichischen und der Schweizer Kollegen haben die Mitglieder des AK DSB die Möglichkeit, in verschiedene Richtungen über den „Tellerrand“ zu schauen: auf der einen Seite in das Nachbarland Österreich, in dem – wie in Deutschland – die DSGVO unmittelbar geltendes Recht ist, und auf der anderen Seite in das Nachbarland Schweiz, die ein eigenes Datenschutzgesetz hat und dem die EU-Kommission in einem sogenannten Angemessenheitsbeschluss gemäß Art. 45 Abs. 3 DSGVO attestiert hat, dass personenbezogene Daten dort einen mit dem Europäischen Datenschutzrecht vergleichbaren adäquaten Schutz genießen.

Des Weiteren hat sich der AK DSB in der Sitzung mit dem seit 1.12.2021 geltenden TTDSG und den praktischen Auswirkungen für die Rundfunkanstalten beschäftigt und sich mit den neuen, von einer Arbeitsgruppe des AK DSB erarbeiteten Leitlinien zum Datenschutz in den Telemedien-Angeboten von ARD, ZDF und Deutschlandradio befasst (s. Kap. C. V. 3.).

Am 31.3.2022 hat der AK DSB zum ersten Mail unter dem Vorsitz des Datenschutzbeauftragten des Bayerischen Rundfunks, Herrn Axel Schneider, getagt. Herr Schneider hat den Vorsitz im Jahr 2022 inne. In dieser virtuellen Sitzung ging es erneut um Abgrenzungsfragen zwischen Auftragsverarbeitung und Joint Controlling, um das geplante gemeinsame SIEM/SOC-System und viele organisatorische Fragen.

K. Rundfunkdatenschutzkonferenz

Die für die Datenschutzaufsicht zuständigen Rundfunkdatenschutzbeauftragten von BR, Deutschlandradio, WDR, SR, ZDF, MDR, NDR und SWR und die Datenschutzbeauftragten des HR, RB, rbb und DW als Aufsichtsbehörden für den journalistisch-redaktionellen Bereich haben sich in der Rundfunkdatenschutzkonferenz (RDSK) zusammengeschlossen.

Zu den Aufgaben der RDSK gehört es insbesondere, die Aufgaben nach Art. 57 DSGVO und die Befugnisse nach Art. 58 DSGVO zu koordinieren und gemeinsame Positionen zu wichtigen datenschutzrechtlichen Fragen zu entwickeln. Im Verhältnis zum AK DSB, der sich auf den

operativen Bereich konzentriert, beschäftigt sich die RDSK mit Grundsatzfragen. Sie kann bei Fragen nach der datenschutzrechtlichen Zulässigkeit vorab konsultiert oder um eine generelle Einschätzung gebeten werden. Eine Geschäftsordnung regelt die wichtigsten Fragen zur Verständigung in Form von Beschlüssen, Entschließungen oder Empfehlungen.

Auf der Internetseite der RDSK (https://www.rundfunkdatenschutzkonferenz.de/) werden die Entschließungen, datenschutzrechtliche Eckpunkte und Positionspapiere der RDSK veröffentlicht.

Unter dem Vorsitz des gemeinsamen Rundfunkdatenschutzbeauftragten von BR, SR, WDR, Deutschlandradio und ZDF, Herrn Dr. Binder, fand am 18.5.2021 eine Videokonferenz mit folgenden Schwerpunktthemen statt:

- Zusammenarbeit mit der DSK,
- Nutzung von Drittplattformen durch die Rundfunkanstalten,
- Aufsichtszuständigkeit bei Kooperationen im Programmbereich und
- Einzelfragen im Zusammenhang mit dem Einsatz von Corona-Warn-Apps

Nachdem Herr Dr. Binder im Januar 2022 vorzeitig den Vorsitz der RDSK niedergelegt hatte, haben die Mitglieder in ihrer Videokonferenz am 29.3.2022 den Rundfunkdatenschutzbeauftragten des MDR, Herrn Stephan Schwarze, mit Wirkung ab diesem Zeitpunkt bis Ende 2022 zum neuen Vorsitzenden der RDSK gewählt. Die rbb-Datenschutzbeauftragte bleibt stellvertretende Vorsitzende der RDSK. Außerdem wurden in der Videokonferenz am 29.3.2022 unter anderem folgende Themen erörtert:

- Bericht aus den Arbeitskreisen der DSK,
- Auslegungsfragen im Zusammenhang mit dem TTDSG und

- Konsequenzen aus dem Urteil des OVG Schleswig-Holstein vom 25.11.2021 zu Facebook Fanpages

L. Zusammenarbeit der datenschutzrechtlichen Aufsichtsbehörden

Entsprechend der föderalen staatlichen Gliederung in Deutschland gibt es neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) jeweils datenschutzrechtliche Aufsichtsbehörden in den einzelnen Bundesländern. Der BfDI ist zuständig für öffentliche Stellen des Bundes und Unternehmen, die Post- bzw. Telekommunikationsdienstleistungen erbringen. Die Zuständigkeit der Aufsichtsbehörden der Länder erstreckt sich auf die öffentlichen Stellen des jeweiligen Landes sowie alle übrigen Unternehmen, die in dem jeweiligen Land ihren Sitz haben. Daneben bestehen auf der Grundlage der Art. 85 Abs. 2 und Art. 91 Abs. 2 DSGVO die Aufsichtsbehörden für die Bereiche Medien (insbesondere Rundfunk) und Kirche.

Nach dem BDSG fällt dem BfDI die Aufgabe zu, auf die Zusammenarbeit der öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, hinzuwirken (§ 16 Abs. 5). Das in § 18 BDSG geregelte Verfahren soll gewährleisten, dass alle Behörden die Regel für das Kohärenzverfahren nach Art. 63 DSGVO einhalten und im Rahmen dessen wirksam beteiligt werden. Die deutschen Aufsichtsbehörden sprechen im Kohärenzverfahren sowie im EDSA mit einer Stimme. Vor der Übermittlung eines gemeinsamen Standpunktes an die Aufsichtsbehörden der anderen Mitgliedsstaaten, die EU-Kommission oder den EDSA geben sich die Aufsichtsbehörden des Bundes und der Länder frühzeitig Gelegenheit zur Stellungnahme (§ 18 Abs. 1 S. 3). Die spezifischen Aufsichtsbehörden für die Bereiche Medien und Kirche werden beteiligt, sofern sie von der Angelegenheit betroffen sind (§ 18 Abs. 1 S. 4).

Die Datenschutzaufsichtsbehörden im öffentlich-rechtlichen Rundfunk sehen die Vorschrift des § 18 Abs. 1 Satz 3 BDSG nur als bedingt geeignet an, die von Art. 63 DSGVO angestrebte Kohärenz zu gewährleisten, denn dem BDSG ist kein Anhaltspunkt dafür zu entnehmen, unter

welchen Voraussetzungen sie von einer entsprechenden Angelegenheit „betroffen“ sein sollen. Aus der DSGVO ergibt sich eine dahingehende Anforderung nicht. Es ist deshalb fraglich, ob sie mit dem Sinn und Zweck der Art. 60 ff. DSGVO vereinbar ist.

Im Mai 2019 hatte die DSK beschlossen, sich regelmäßig zweimal jährlich mit den sogenannten spezifischen Aufsichtsbehörden auszutauschen. Zu den spezifischen Aufsichtsbehörden gehören neben den Rundfunkdatenschutzbeauftragten auch Datenschutzbeauftragte der Medienanstalten und die Datenschutzbeauftragten der Kirchen. Unter der Leitung der Landesbeauftragten für Datenschutz und Informationsfreiheit Saarland, Monika Grethel, fanden am 5.5.2021 und 8.12.2021 Videokonferenztermine zum Austausch mit den spezifischen Aufsichtsbehörden statt. Wie schon im letzten Tätigkeitsbericht erwähnt, hat die DSK auch ihre Arbeitskreise für die spezifischen Aufsichtsbehörden geöffnet. Allerdings lassen die Arbeitskreise eine Beteiligung der Vertreter:innen der RDSK nur auf Basis eines Gaststatus zu. Leider werden die spezifischen Aufsichtsbehörden bislang auch nicht an der Erarbeitung von Orientierungshilfen und Entschließungen beteiligt, so dass eine gemeinsame inhaltliche Auseinandersetzung mit datenschutzrechtlichen Einzelfragen bislang kaum stattgefunden hat. Es bleibt zu hoffen, dass die Beteiligten in Zukunft über eine gegenseitige Information hinaus zu einer echten Zusammenarbeit kommen. Seit Anfang 2022 hat der BfDI den Vorsitz der DSK inne.

M. Teilnahme an Fortbildungen und Veranstaltungen

Zur Erhaltung und Erweiterung meines Fachwissens habe ich an folgenden Veranstaltungen teilgenommen:

- Datentag Online der Stiftung Datenschutz zum Thema „3 Jahre DSGVO“ am 25.5.2021
- Online-Kompaktkurs der Fa. Datakontext „Die neuen EU-Standardvertragsklauseln“ am 26.8.2021
- Online-Veranstaltung der Stiftung Datenschutz „Datenpolitik der Europäischen Kommission: Data Governance Act, Data Act, Datenräume und mehr“ am 6.10.2021

- Online-Kurs der Gesellschaft für Datenschutz und Datensicherheit mbH „Tracking online – Neues Online-Datenschutzrecht ab Dezember 2021“ am 8.11.2021

- Online-Veranstaltung der Stiftung Datenschutz „Faires Internet-Marketing, Tracking Datenschutz“ am 7.12.2021

- Online-Veranstaltung des Instituts für Europäisches Medienrecht „Gesetz über digitale Märkte (DMA) vor dem Trilog“ am 18.1.2022

- Online-Veranstaltung Anwaltskanzlei Taylor Wessing „Ausblick 2022 aus Sicht der Datenschutzbehörden“ (u. a. mit dem Landesbeauftragten für Datenschutz und die Informationsfreiheit des Landes Rheinland-Pfalz) am 26.1.2022

- Online-Seminar der Fa. Ditis zur Zertifizierung nach ISO 27701 (Informationssicherheit und Datenschutz)

Berlin, 1.6.2022

gez. Anke Naujock-Simon

Anlage:

Leitlinien zum Datenschutz in den Telemedien-Angeboten von ARD; ZDF und Deutschlandradio