16. Tätigkeitsbericht

der Beauftragten für den Datenschutz

des

Rundfunk Berlin-Brandenburg

Berichtszeitraum:

01. April 2019 bis 31. März 2020

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
AFPS	Audiofingerprintingsystem
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BlnDSG	Berliner Datenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informations-Technik
BR	Bayerischer Rundfunk
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
DSAnpUG	Datenschutz-Anpassungs- und Umsetzungsgesetz
DSFA	Datenschutz-Folgenabschätzung
DLR	Deutschlandradio
DSGVO	EU-Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz der unabhängigen Daten-schutzaufsichtsbehörden des Bundes und der Länder
DW	Deutsche Welle
ems	Eletronic Media School
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FS	Freienstatut
FSZ	Fernsehzentrum
GeschGehG	Geschäftsgeheimnisgesetz
GO	Geschäftsordnung
HA	Hauptabteilung
HdR	Haus des Rundfunks

HR	Hessischer Rundfunk
HSB	ARD-Hauptstadtstudio
IVZ	Informationsverarbeitungszentrum
LG	Landgericht
MDR	Mitteldeutscher Rundfunk
MIT	Hauptabteilung Mediensysteme und IT
MoWaS	modulares Warn-System des Bundes
NDR	Norddeutscher Rundfunk
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
POC	ARD-Play-Out-Center
PWC	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
OUI	Abteilung Organisation und IT
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
RGebStV	Rundfunkgebührenstaatsvertrag
RBT	Arbeitsgemeinschaft Rundfunk-Betriebstechnik
RDSK	Rundfunkdatenschutzkonferenz
RStV	Rundfunkstaatsvertrag
SR	Saarländischer Rundfunk
SWR	Südwestrundfunk
TMG	Telemediengesetz
VG	Verwaltungsgericht
VPMS	Video Production Management Suite
VVT	Verzeichnis von Verarbeitungstätigkeiten

WDR	Westdeutscher Rundfunk
ZBS	Zentraler Beitragsservice
zibb	Zuhause in Berlin & Brandenburg

Vorbemerkung

Mit diesem Tätigkeitsbericht wird die Entwicklung des Datenschutzes beim Rundfunk Berlin-Brandenburg (rbb) für die Zeit vom 01.04.2019 bis 31.03.2020 dokumentiert. Der Tätigkeitsbericht umfasst meine Aktivitäten als Beauftragte für den Datenschutz im journalistisch-redaktionellen Bereich und als betriebliche Datenschutzbeauftragte im wirtschaftlich-administrativen Bereich.

Seit Juli 2019 bin ich hauptamtlich Datenschutzbeauftragte und als unabhängige Stabsstelle der Intendanz angegliedert. Vor dem Hintergrund der gestiegenen Bedeutung des Datenschutzes und der neu hinzugekommenen Aufgaben nach Wirksamwerden der EU-Datenschutzgrundverordnung (DSGVO) im Mai 2018 hatte die Intendantin im Frühjahr 2019 entschieden, die Funktion der Datenschutzbeauftragten zukünftig hauptamtlich zu besetzen und direkt in der Intendanz anzusiedeln. Bis zu diesem Zeitpunkt hatte ich die Funktion nebenamtlich zu meinen Aufgaben als juristische Mitarbeiterin im Justitiariat wahrgenommen. Mit der Herauslösung des Amts aus dem Justitiariat wurde die von der DSGVO geforderte „völlige Unabhängigkeit“ der Datenschutzbeauftragten auch formal hergestellt. Die ersten Monate im Hauptamt haben gezeigt, dass die Entscheidung der Intendantin zur richtigen Zeit kam. Der Aufgabenumfang wäre im Nebenamt rein quantitativ überhaupt nicht mehr zu bewältigen gewesen.

Im Berichtszeitraum bildete die Neuorganisation des Datenschutz-Bereiches einen Schwerpunkt meiner Arbeit. Das zuvor gemeinsam mit dem Justitiariat genutzte Dokumentenmanagement-System wurde auf meine Veranlassung hin getrennt. Diese Trennung hat zur Folge, dass der Datenschutz nunmehr eine separate Datenhaltung und Administration des Systems für seinen Bereich durchführt. Die organisatorische Selbständigkeit der Datenschutzbeauftragten und die veränderten Anforderungen der DSGVO haben auch die Festlegung völlig neuer Workflows erforderlich gemacht. Zusätzlich zu diesen Herausforderungen galt es, eine schwierige räumliche Situation zu bewältigen. Aufgrund der generellen Raumknappheit im rbb konnten für die

Datenschutzbeauftragte und ihren Assistenten zunächst keine zusammenhängenden Räume gefunden werden. Dies hatte zur Folge, dass ich bis März 2020 weiterhin in meinem angestammten Büro im Justitiariat im Fernsehzentrum (FSZ) am Theodor-Heuß-Platz in Berlin saß (und damit den Raum für meine Nachfolgerin im Justitiariat blockiert habe). Für meinen Assistenten war nach längerer Suche ein kleiner Raum im Haus des Rundfunks (HdR) gefunden worden. Dieser unbefriedigende Zustand, der mit vielen täglichen Gängen zwischen HdR und FSZ für meinen Mitarbeiter und mich verbunden war, hat im April 2020 ein Ende gefunden. Zusammen mit Kolleg*innen aus den Abteilungen Personalstrategie und -entwicklung, Personalmanagement, Lizenzen und Rechnungswesen ist der Bereich Datenschutz für ca. 14 Monate an den neuen Standort des rbb am Saatwinkler Damm umgezogen. (Die Errichtung dieses neuen Standortes war für den rbb wegen der geplanten Umbaumaßnahmen im FSZ für das zukünftige Crossmediale Newscenters erforderlich geworden.) Richtig einleben konnten wir uns dort bislang allerdings nicht: Wegen der Corona-Pandemie befinden sich die Datenschutzbeauftragte und ihr Mitarbeiter – wie alle anderen nicht senderelevanten Bereiche - seit Mitte März überwiegend im Homeoffice.

Einen weiteren Schwerpunkt bildete im Berichtszeitraum Restarbeiten im Zusammenhang mit der Umsetzung der DSGVO. Das betrifft u.a. die Anpassung von internen Regelwerken und die Überarbeitung von Vertragsmustern, Formularen und Fragebögen sowie die Erarbeitung von bereichsspezifischen Löschkonzepten. Das neue Verarbeitungsverzeichnis (VVT) gemäß Art. 30 DSGVO, in dem alle Verfahren mit personenbezogenen Daten dokumentiert werden müssen, wurde weiter aufgebaut.

Das Thema Datensicherheit nimmt im rbb stetig an Bedeutung zu. Der Aufwand für die Beseitigung und Abwehr von Angriffen auf unser Netzwerk wird kontinuierlich größer, da immer häufiger auch die Netzwerke öffentlicher Einrichtungen Ziele von Hackerangriffen sind. Als einer der spektakulärsten Fälle in Berlin ist sicherlich der Angriff im September 2019 auf das Computersystem des Kammergerichts zu nennen. Der rbb ist vergleichsweise gut aufgestellt. Die im rbb eingesetzte Software ist

aktuell und bietet daher vergleichsweise wenig Angriffsfläche. Mittels spezieller Software konnten zudem die kleineren Angriffe, die es gegenüber dem rbb im Berichtszeitraum gab, von den Kollegen aus der IT frühzeitig entdeckt und abgewehrt werden. Und auch organisatorisch haben wir weitere Verbesserungen erreichen können. Datenschutz und Informationssicherheit wurden noch enger als bislang verzahnt. Im Rahmen der regelmäßig stattfindenden Schulungen zu Datenschutz und Informationssicherheit sensibilisieren der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte gemeinsam für die Gefahren durch Hackerangriffe. Dabei geben wir konkrete Tipps zum Verhalten am Arbeitsplatz. Selbstverständlich ist uns bewusst, dass wir mit allen im rbb ergriffenen technischen und organisatorischen Maßnahmen die Angriffsrisiken niemals gänzlich ausschließen können.

Die Vielzahl der Einzelvorgänge, mit denen die Datenschutzbeauftragte im Berichtszeitraum befasst war, macht es erforderlich, sich in diesem Tätigkeitsbericht auf die Darstellung von grundsätzlichen und exemplarischen Einzelfragen zu beschränken.

Meinem Mitarbeiter Christoph Schneider und meinem Stellvertreter Herrn Axel Kauffmann sowie dem Informationssicherheitsbeauftragten Michael Kalisch und seinem Mitarbeiter Marcel Kuring danke ich für intensive und produktive Zusammenarbeit im zurückliegenden Jahr. Dank gebührt auch in diesem Jahr wieder dem Personalrat für die vertrauensvolle Kooperation.

Bei der Bewältigung von schwierigen Situationen und Entscheidungen konnte ich mir der Rückendeckung seitens der Intendanz stets gewiss sein. Alle meine Wünsche bezüglich räumlicher und personeller Ausstattung sowie Arbeitsmaterialien und Fortbildungen wurden prompt erfüllt. Auch dadurch wurde mir das Gefühl vermittelt, dass meine Arbeit geschätzt wird. Dafür möchte ich mich herzlich bedanken.

Dieser Tätigkeitsbericht wird – wie die Vorgängerberichte - im Online-Angebot des rbb veröffentlicht.

Er wird unter

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

abrufbar sein.

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. Der oder die Beauftragte für den Datenschutz ist in Ausübung seines/ihres Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er/sie der Dienstaufsicht des Verwaltungsrates.

Gemäß Abs. 2 Satz 2 überwacht er/sie die Einhaltung der Datenschutzvorschriften des rbb-Staatsvertrages und anderer Vorschriften über den Datenschutz, soweit der rbb personenbezogene Daten zu eigenen, journalistisch-redaktionellen oder literarischen Zwecken verarbeitet. Konkretisiert werden die Aufgaben und Befugnisse der Rundfunkdatenschutzbeauftragten nunmehr durch Art. 51 ff. DSGVO.

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 außerdem – wie bei allen Berliner Behörden und sonstigen öffentlich-rechtlichen Stellen – eine/ein betriebliche/r Datenschutzbeauftragte/r sowie jeweils eine/ein Stellvertreterin/Stellvertreter zu bestellen. Diese Pflicht ergibt sich aus § 36 Abs. 1 rbb-StV i. V. m. § 4 Abs. 1 Berliner Datenschutzgesetzes (BlnDSG).

Gemäß Art. 57 DSGVO haben die datenschutzrechtlichen Aufsichtsbehörden – und damit auch die rbb-Datenschutzbeauftragte im journalistisch-redaktionellen Bereich - u. a. folgende Aufgaben:

- Überwachung der Einhaltung der DSGVO,
- Beratung, Aufklärung und Sensibilisierung der Öffentlichkeit und der Verantwortlichen 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 betriebliche Datenschutzbeauftragte – und damit auch die rbb-Datenschutzbeauftragte im wirtschaftlich-administrativen Bereich - mindestens folgende Aufgaben zu erfüllen:

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

Gegenüberstellung der Aufgaben der Aufsichtsbehörde und des betrieblichen Datenschutzbeauftragten, dessen Kompetenzen durch die DSGVO erweitert wurden („Überwachung", anstatt wie zuvor „Hinwirken auf die Einhaltung der Datenschutzgesetze"), zeigt viele Überschneidungen. Das bedeutet für die Datenschutzbeauftragte des rbb, dass es bei der täglichen Arbeit kaum einen Unterschied macht, ob sie in der einen oder anderen Funktion tätig wird, zumal sie oftmals auch im wirtschaftlich-administrativen Bereich von den Mitarbeiterinnen und Mitarbeitern und Geschäftspartnern als erste Anlaufstelle für datenschutzrechtliche Beschwerden gesehen wird.

II. Konkrete Situation

Auf seiner Sitzung am 20.06.2019 hat mich der Rundfunkrat gemäß § 38 Abs. 1 rbb-StV auf Vorschlag der Intendantin für eine weitere Amtszeit von vier Jahren für den Zeitraum 01.07.2019 bis 30.06.2023 zur Beauftragten für den Datenschutz bestellt. Parallel dazu hat mich die Intendantin für den gleichen Zeitraum zur betrieblichen Datenschutzbeauftragten gemäß § 4 Abs. 1 BlnDSG bestellt. 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 01.07.2019 das Amt der Compliancebeauftragten.

Seit dem 01.04.2014 ist Herr Axel Kauffmann stellvertretender betrieblicher Datenschutzbeauftragter. Herr Kauffmann war bis Ende August 2019 Mitarbeiter der internen Revision. Seit 01.09.2019 leitet er diese Abteilung. Trotz der dadurch bedingten höheren Arbeitsbelastung hat sich Herr Kauffmann bereit erklärt, auch weiterhin als stellvertretender betrieblicher Datenschutzbeauftragter zur Verfügung zu stehen. Während ich Herrn Kauffmann in den zurückliegenden Jahren bei größeren Projekten fortlaufend mit einbeziehen konnte, steht er inzwischen aufgrund dieser neuen Tätigkeit im Wesentlichen nur noch als Abwesenheitsvertreter zur Verfügung.

Zusätzlich hat er auch im Berichtszeitraum wieder eine Reihe von Datenschutzschulungen durchgeführt (s. G.)

Seit August 2018 hat die Datenschutzbeauftragte Unterstützung durch einen Assistenten. Herr Christoph Schneider erledigt Sekretariatsarbeit und entlastet mich bei der Routine-Sachbearbeitung. Ab Juli 2020 wird die rbb-Datenschutzbeauftragte auch eigene Rechtsreferendare ausbilden.

B. Entwicklung des Datenschutzrechts

I. Europa

1. Normen und Abkommen

1.1 EU-Datenschutzgrundverordnung

Seit 25.05.2018 ist die EU-Datenschutzgrundverordnung (DSGVO) in allen Mitgliedsstaaten der Europäischen Union (EU) unmittelbar geltendes Recht. Zu den Rechtsfolgen habe ich zuletzt im 15. Tätigkeitsbericht Stellung genommen (S. 11 ff.) Für konkrete Umsetzungsfragen im Zusammenhang mit der DSGVO ist u.a. die Rechtsprechung des Europäischen Gerichtshofs (EuGH) maßgeblich (s. dazu 2.).

1.2 ePrivacy-Verordnung

Wie im 15. Tätigkeitsbericht erwähnt (S. 12 ff.) soll die ePrivacy-Verordnung Vorgaben zum Datenschutz bei der Bereitstellung und Nutzung von Telemediendiensten, klassischen Kommunikationsdiensten wie Telefonie und SMS und internetbasierten Kommunikationsdiensten, insbesondere Messenger wie Skype oder WhatsApp regeln. Ursprünglich war geplant, zeitgleich mit der DSGVO auch die ePrivacy-Verordnung in Kraft treten zu lassen. Leider ist dies nicht geschehen. Die Mitglieder der EU konnten sich bis heute nicht auf deren Inhalt einigen. Dies ist besonders misslich, weil sich durch dieses Regelungsvakuum viele Rechtsfragen stellen – u. a. im Zusammenhang mit dem Webtracking, das auch für den rbb relevant ist. Eine zeitnahe Klärung dieser höchst umstrittenen Rechtsfragen durch die Verabschiedung der ePrivacy-Verordnung wäre wünschenswert.

1.3 Whistleblower-Richtlinie

Die EU hat am 23.10.2019 die Richtlinie 2019/1937 „zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden" erlassen (sog. Whistleblower-Richtlinie). Sie wurde am 26.11.2019 im Amtsblatt veröffentlicht und muss von den Mitgliedstaaten bis zum 17.12.2021 in nationales Recht umgesetzt werden. Wie sich aus dem Erwägungsgrund 14 ergibt, wird die Meldung von Hinweisgebern als besonders nützlich angesehen, wenn dadurch Sicherheitsvorfälle oder Verstöße gegen die Datenschutzvorschriften der EU verhindert werden. Deshalb sollen beispielsweise auch Hinweise von Informanten im Hinblick auf die DSGVO durch diese Vorschrift geschützt werden.

1.4 Privacy Shield

Der sog. „Privacy Shield" gestattet es US-amerikanischen Unternehmen, Daten europäischer Bürger zu verarbeiten, wenn sie sich gegenüber dem US-Handelsministerium dazu verpflichten, dessen Datenschutzgrundsätze anzuerkennen und sie sich entsprechend zertifizieren lassen. Dieses transatlantische Datenschutzabkommen ist hoch umstritten und auch gerichtlich angefochten. Zwar schafft der Privacy Shield gegenüber dem früheren Safe-Harbor-Abkommen verbesserte Datenschutzbedingungen. Es gibt aber nach wie vor Regelungslücken. Dennoch hat die EU-Kommission auch Ende 2019 in ihrer jährlichen Überprüfung erneut festgestellt, dass unter dem Regime des Privacy Shield ein angemessenes Datenschutzniveau herrsche. Der Privacy Shield steht auf dem Prüfstand beim EuGH. Eine Entscheidung ergeht voraussichtlich noch in der ersten Jahreshälfte 2020 (s. dazu 2.5).

2. Entscheidungen

2.1 Urteil des EuGH zum „Like"-Button

Der EuGH hat zum „Gefällt-mir" bzw. „Like"-Button von Facebook am 29.07.2019 eine grundsätzliche Entscheidungen getroffen (AZ.: C-40/17 – Fashion ID) Dieser Entscheidung lag folgender Sachverhalt zugrunde: Fashion ID, ein Online-Händler für Modeartikel, hatte im Jahre 2015 auf seiner Webseite das Plugin „Gefällt mir" bzw. „Like"-Button des sozialen Netzwerks Facebook eingebunden. Diese Einbindung hatte zur Folge, dass beim Aufrufen der Webseite von Fashion ID automatisch die personenbezogenen Daten des Nutzers an Facebook Irland übermittelt wurden. Die Übermittlung erfolgte, ohne dass sich der Nutzer dessen bewusst war und unabhängig davon, ob er Mitglied des sozialen Netzwerks Facebook war, oder den „Gefällt mir"-Button angeklickt hatte.

Die Verbraucherzentrale Nordrhein-Westfalen (NRW) erhob gegen Fashion ID beim Landgericht (LG) Düsseldorf Klage auf Unterlassung und erhielt teilweise recht. Die Sache ging in die Berufungsinstanz zum Oberlandesgericht (OLG) Düsseldorf. Das OLG Düsseldorf setzte das Berufungsverfahren aus und legte dem EuGH mehrere Fragen zur Vorabentscheidung vor.

Die wesentlichen Aussagen des EuGH-Urteils:

Neben den Datenschutzbehörden und den eigentlich Betroffenen können Verbraucherverbände im Fall von Datenschutzverletzungen gegen den Verletzer vorgehen. (Die Entscheidung erging noch zur alten Datenschutzrichtlinie 95/46/EG. Mit der Geltung der DSGVO ist diese Frage mittlerweile gesetzlich geklärt, denn Art. 80 Abs. 2 DSGVO sieht diese Möglichkeit nun ausdrücklich vor.)

Fashion ID kann für die Vorgänge des Erhebens der in Rede stehenden Daten und deren Weiterleitung durch Übermittlung an Facebook Irland als gemeinsam mit

Facebook verantwortlich angesehen werden, da (vorbehaltlich der vom OLG vorzunehmenden Nachprüfung) davon ausgegangen werden kann, dass Fashion ID und Facebook Irland gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Fashion ID habe über die Mittel durch Einbindung des „Like"-Buttons entschieden.

Offengelassen hat der EuGH die Frage, ob die Verwendung von Social Plugins immer einer Einwilligung bedarf. Darüber muss nun das OLG Düsseldorf befinden. Das Gericht hat die Aufgabe festzustellen, welche Rechtsgrundlage (berechtigte Interessen oder Einwilligung) tatsächlich im Falle der Verwendung des „Like"-Buttons erforderlich ist. Der EuGH hat für beide möglichen Fälle die Verantwortlichkeiten geklärt: Sollte der Einsatz des „Like-„Buttons auf die berechtigten Interessen gemäß Art. 6 Abs. 1 f DSGVO gestützt werden können, muss jeder der Verantwortlichen (Fashion ID und Facebook) jeweils ein eigenes berechtigtes Interesse vorweisen können. Sollte hingegen eine Einwilligung erforderlich sein, müsste der Webseitenbetreiber die Einwilligung für die Erhebung und Weiterleitung der personenbezogenen Daten einholen. Facebook müsste demgegenüber eine Einwilligung für die anschließende Verarbeitung der Webseitenbesucherdaten einholen.

Diese Aussagen des EuGH sind auf alle Social-Media-Plugins übertragbar. Für den rbb gibt es nach dem Urteil allerdings keinen unmittelbaren Handlungsbedarf, da er in seinen Telemedienangeboten seit langem eine sog. Zwei-Klick-Lösung implementiert hat. Das bedeutet, dass die Buttons zu den Social Media Kanälen in die Web-Angebote des rbb ohne eine automatische Verbindung zu den Social-Media-Anbietern integriert sind. Erst mit Anklicken eines Buttons wird eine Verbindung hergestellt.

2.2 Urteil des EuGH zur wirksamen Erteilung einer Einwilligung für Cookies

Mit Urteil vom 01.10.2019 (C-673/17) hat der EuGH in der Sache „Planet 49" die Anforderungen an eine wirksame Einwilligung zur Speicherung von Informationen oder zum Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer

Webseite gespeichert sind, konkretisiert. Danach reicht ein voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, nicht aus. Es mache insoweit keinen Unterschied, ob es sich bei den im Gerät des Nutzers gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt oder nicht. Das Unionsrecht soll den Nutzer nämlich vor jedem Eingriff in seine Privatsphäre schützen, insbesondere gegen die Gefahr, dass „Hidden Identifiers" (= versteckte Kennungen) oder ähnliche Instrumente in sein Gerät eindringen. Der EuGH stellt ferner klar, dass der Diensteanbieter gegenüber dem Nutzer u.a. auch Angaben zur Funktionsdauer der Cookies und zur Zugriffsmöglichkeit Dritter machen muss.

Das Urteil hat vermehrt zu Fragen der Zulässigkeit des Einsatzes von Cookies in den Online-Angeboten der Rundfunkanstalten geführt, wenngleich darüber gar nicht entschieden wurde. Zur Klarstellung hat die Rundfunkdatenschutzkommission (RDSK) daher in einem Positionspapier die Rechtslage zusammengefasst (Anlage 4). Danach ergibt sich Folgendes:

Nach Art. 6 der EU-Datenschutz-Grundverordnung kann der Einsatz von Cookies über eine Einwilligung oder über andere Erlaubnistatbestände gerechtfertigt sein.
Eine Einwilligung ist nicht nötig, wenn die mit dem Einsatz des Cookies verbundene Speicherung oder der Zugang zu den entsprechenden Daten unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Danach bedürfen jedenfalls sogenannte ‚funktionale Cookies' keiner Einwilligung, die etwa dem Verantwortlichen eine (technische) Fehleranalyse ermöglichen, der Sicherheit seines Angebots dienen, die Login-Daten seiner Nutzer speichern, für Transaktionen (Warenkorbfunktion) oder zur Individualisierung von Webseiteninhalten erforderlich sind.

Die in den Telemedienangeboten des öffentlich-rechtlichen Rundfunks praktizierte anonyme Nutzungsmessung stützt sich auf die Rechtsgrundlagen Art. 6 Abs. 1 S. 1 lit. e) bzw. f) DSGVO und bedarf daher ebenfalls keiner Einwilligung.

Der öffentlich-rechtliche Rundfunk verbreitet Telemedien, um seinen verfassungsrechtlichen Funktionsauftrag zu erfüllen. Nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) darf (und muss) er sein von den Beitragszahlern finanziertes Angebot im gesellschaftlichen Interesse auf allen publizistisch relevanten Plattformen zugänglich machen. Ob, wo und wie er damit seinen publizistischen Auftrag erfüllt, hängt von der Konfiguration dieses Angebots ab. Die Rundfunkanstalten sind dazu auf Erkenntnisse zur Akzeptanz und Nutzung ihres Angebots angewiesen. Dies gilt allerdings ausschließlich für anonyme Auswertungen, wie sie auch im linearen Rundfunk üblich sind. Vergleichbar statistisch belastbare Methoden wie etwa die Messung der Zuschauerquoten (Fernsehen) oder die Media-Analyse (Hörfunk) stehen dafür im Online-Bereich bislang nicht zur Verfügung. Die Rundfunkanstalten haben daher im Rahmen ihres verfassungsrechtlichen Funktionsauftrags ein berechtigtes Interesse am Einsatz von Cookies, die diese Aufgabe für ihr Onlineangebot übernehmen.

2.3 Urteil des EuGH zur Verpflichtung zur Arbeitszeiterfassung

Mit Urteil vom 14.05.2019 (C-55/18) hat der EuGH entschieden, dass die Mitgliedstaaten Arbeitgeber dazu verpflichten müssen, ein System einzurichten, mit dem die tägliche Arbeitszeit der Mitarbeiter gemessen werden kann. Die Mitgliedstaaten müssten alle erforderlichen Maßnahmen treffen, dass den Arbeitnehmern die täglichen und wöchentlichen Mindestruhezeiten und die Obergrenze für die durchschnittliche wöchentliche Arbeitszeit der Arbeitszeitrichtlinie tatsächlich zugutekommen. Nur so könne der durch die EU-Grundrechtecharta und die Arbeitszeitrichtlinie bezweckte Gesundheitsschutz der Arbeitnehmer tatsächlich einer Kontrolle durch Behörden und Gerichte zugeführt werden. Die gesamte Arbeitszeit sei vollständig zu dokumentieren.

Diese Entscheidung des EuGH ist ein Rückschritt für die digitale Arbeitswelt. Homeoffice und mobiles Arbeiten haben – auch vor dem Hintergrund von „Corona“ - inzwischen Einzug auch in den Arbeitsalltag der meisten rbb-Mitarbeiterinnen und Mitarbeiter gefunden. Durch die Verpflichtung zur aktiven Zeiterfassung könnte diese neue Flexibilität wieder stark eingegrenzt werden.

Abzuwarten bleibt, wie der deutsche Gesetzgeber die Verpflichtung zur Arbeitszeiterfassung umsetzen wird. Jedenfalls bis zur Verabschiedung eines entsprechenden Gesetzes besteht für den rbb kein Handlungsbedarf.

2.4 Urteile des EuGH zum "Recht auf Vergessen"

Schon vor rund sechs Jahren hat der EuGH entschieden, dass Suchmaschinenbetreiber verpflichtet sind, Suchergebnisse zu löschen, wenn diese Persönlichkeitsrechte europäischer Bürger verletzen. Mit Urteil vom 24.09.2019 (C-507/17) hat der EuGH sein Grundsatzurteil nun präzisiert und sich zur geografischen Reichweite des sog. Auslistungsanspruchs geäußert. Demnach ist ein Suchmaschinenbetreiber nach EU-Recht nicht verpflichtet, das "Recht auf Vergessen" außerhalb der EU-Mitgliedsländer zu realisieren. Die Suchergebnisse müssen lediglich in allen europäischen Versionen der Suchmaschine ausgelistet werden. Weiterhin hat der Suchmaschinenbetreiber verlässliche Maßnahmen zu ergreifen, die verhindern, dass Internetnutzer von Mitgliedstaaten aus mit Hilfe einer Nicht- EU-Version der Suchmaschine auf die personenbezogenen, ausgelisteten Verlinkungen zugreifen.

In einem weiteren Urteil desselben Tages (C-136/17) hat sich der EuGH zur Verantwortung des Betreibers einer Suchmaschine im Umgang mit personenbezogenen Daten besonderer Kategorien i. S. von Art. 9 DSGVO geäußert. Das sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischer Daten zur eindeutigen

Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Der EuGH hat eine grundsätzliche Auslistungspflicht von Suchmaschinenbetreibern in Bezug auf solche Links verneint, die zu Webseiten mit besonders sensiblen personenbezogenen Daten führen. Allerdings hat er zugleich die Pflicht des Anbieters statuiert, im Falle des Löschantrags eines Betroffenen zu prüfen, ob die Aufnahme des entsprechenden Links in die Liste der Suchergebnisse unbedingt erforderlich ist, um das Recht auf Informationsfreiheit der anderen Nutzer zu schützen (s. dazu Art. 9 Abs. 2 lit. g) DSGVO). Darüber hinaus hat der EuGH die Anforderungen in Bezug auf die Veröffentlichung von Informationen zu einem Strafverfahren präzisiert. Einem Antrag auf Auslistung sei immer dann stattzugeben, wenn sich die Informationen auf einen früheren Verfahrensabschnitt beziehen und nicht mehr der aktuellen Situation entsprechen. Selbst wenn dem Antrag nicht stattgegeben wird, sei der Suchmaschinenbetreiber verpflichtet, den Antrag zum Anlass zu nehmen, seine Suchergebnisliste so auszugestalten, dass sich daraus für den Suchmaschinennutzer das Gesamtbild der aktuellen Rechtslage widerspiegelt.

2.5 EuGH-Verfahren zur Zulässigkeit des Datentransfers in die USA

Im Jahr 2015 erreichte der österreichische Jurist Max Schrems mit seiner Klage gegen Facebook, dass der EuGH das sog. Safe-Harbor-Abkommen der EU-Kommission für ungültig erklärte. Bis dahin hatte die EU anerkannt, dass US-Unternehmen, die sich den Safe-Harbor-Prinzipien unterwarfen, ausreichenden Datenschutz garantieren. An diese Unternehmen durften danach Daten aus der EU geschickt werden. Der EuGH konstatierte, dass für einen Datentransfer in die USA der Datenschutz gleichwertig mit dem in der EU sein müsse. Die EU-Kommission habe das Datenschutzniveau in den USA gar nicht hinreichend geprüft. Daher müssten die nationalen Datenschutzbeauftragten "mit aller gebotenen Sorgfalt" und anhand genauer Kriterien prüfen, ob die übermittelten Daten in den USA ausreichend geschützt werden. Daraufhin teilte die für Facebook zuständige irische Datenschutzbehörde Max Schrems

Ende 2015 mit, Facebook habe die Übermittlung der Daten in die USA von Anfang an nicht auf Grundlage des Safe-Harbor-Abkommens vorgenommen, sondern auf Grundlage sog. Standardvertragsklauseln. Das sind von der EU-Kommission anerkannte Formulierungen, mit denen Unternehmen die Einhaltung ausreichender Datenschutzstandards garantieren können. Aufgrund dieser Garantien genehmigen die Datenschutzbehörden Datenübertragungen auch in Staaten ohne angemessenes Datenschutzniveau. Dieses Verfahren greift Schrems mit seiner aktuellen Klage nicht an. Seine neuerliche Klage richtet sich vielmehr dagegen, dass Unternehmen gegen ihre eigenen Garantien in den Standardvertragsklauseln verstoßen könnten. Er hat darauf hingewiesen, dass Facebook nach den US-Gesetzen die Daten – wenn gefordert – auch gegen den Willen der Nutzer den amerikanischen Ermittlungsbehörden zugänglich machen müsste. Außerdem geht es in dem neuen Verfahren auch um das Nachfolgeinstitut zum Safe Harbor-Abkommen, dem Privacy-Shield (s. dazu 1.4).

Gemäß dem Schlussantrag des EuGH-Generalanwaltes vom 19.12.2019 können die aktuellen Regeln für Datentransfers aus Europa vermutlich in Kraft bleiben. Der Beschluss der Kommission über die Standardvertragsklauseln ist nach seiner Auffassung gültig. Die Verantwortlichen für die Datenverarbeitung und die Kontrollbehörden seien allerdings verpflichtet, die Übermittlung zu stoppen, wenn gegen Datenschutz-Vorgaben verstoßen werde. Der Generalanwalt stellte zunächst fest, dass es im Ausgangsrechtsstreit nur um die Feststellung gehe, ob der Beschluss 2010/87 gültig sei, mit dem die Kommission die Standardvertragsklauseln festgelegt hat, die für die in der Beschwerde von Schrems genannten Übermittlungen geltend gemacht worden seien. Nach Auffassung des Generalanwaltes führt der Umstand, dass der Beschluss und die darin enthaltenen Standardvertragsklauseln die Behörden des Drittbestimmungslandes nicht binden, für sich allein nicht zur Ungültigkeit des Beschlusses. Die Wirksamkeit des Beschlusses hänge vielmehr davon ab, ob ausreichend wirksame Regelungen bestünden, mit denen sich sicherstellen lasse, dass die auf die Standardvertragsklauseln gestützten Übermittlungen ausgesetzt oder verboten würden, wenn die Klauseln verletzt würden oder es unmöglich ist, sie einzuhalten. Dies sei dann der Fall, wenn eine Pflicht – der für die Datenverarbeitung

Verantwortlichen und, bei deren Untätigkeit, der Kontrollstellen – bestehe, eine Übermittlung auszusetzen oder zu verbieten, wenn aufgrund eines Konflikts zwischen den sich aus den Standardvertragsklauseln ergebenen Pflichten und den durch das Recht des Drittbestimmungslandes auferlegten Pflichten diese Klauseln nicht eingehalten werden könnten.

Für die Entscheidung über den Ausgangsrechtsstreit hält es der Generalanwalt nicht für erforderlich, dass der EuGH über die Gültigkeit des Privacy-Shield entscheidet, da der Rechtsstreit nur die Gültigkeit des Beschlusses zu den Standardvertragsklauseln betreffe. Gleichwohl führt der Generalanwalt in seinem Schlussantrag auch aus, aus welchen Gründen sich für ihn im Hinblick auf die Rechte auf Achtung des Privatlebens, auf Schutz personenbezogener Daten und auf einen wirksamen Rechtsbehelf Fragen bezüglich der Gültigkeit des Privacy-Shields stellen.

II. Bund

1. Normen

1.1 Zweites Gesetz zur Anpassung des Datenschutzrechts an die DSGVO

Zum 26.11.2019 sind mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU („2. DSAnpUG-EU") Änderungen im Bundesdatenschutzgesetz (BDSG) und in zahlreichen bereichsspezifischen Gesetzen in Kraft getreten. Es wurden insbesondere Begriffsbestimmungen, Verweisungen, Rechtsgrundlagen, Betroffenenrechte und Vorgaben zu technischen und organisatorischen Maßnahmen angepasst bzw. neu geregelt. Für den rbb besonders relevant ist die Regelung in § 26 Abs. 2 S. 3 BDSG n.F.. Danach muss die Einwilligung im Beschäftigtenkontext nunmehr nicht mehr zwingend grundsätzlich schriftlich, sondern kann auch ohne besondere Begründung in elektronischer Form erteilt werden. Außerdem wurde mit dem 2. DSAnpUG-EU auch das Deutsche-Welle-Gesetz geändert und die sog. gespaltene Kontrollzuständigkeit neu eingeführt. Der Rundfunkdatenschutzbeauftragte der Deutschen

Welle (DW) ist jetzt – wie schon bislang die Datenschutzbeauftragten von Radio Bremen (RB), Hessischem Rundfunk (HR) und rbb - nur noch für den journalistisch-redaktionellen Bereich Aufsichtsbehörde i. S. d. DSGVO. Ansonsten unterliegt die DW der Aufsicht des Bundesdatenschutzbeauftragten.

1.2 Gesetz zum Schutz von Geschäftsgeheimnissen

Seit 26.04.2019 ist das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) in Kraft (s. dazu auch 15. Tätigkeitsbericht, S. 22 f.). Damit wurde die europäische „Richtlinie 2016/943 zum Schutz vertraulichen Know-hows und Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung“ in nationales Recht umgesetzt.

Von besonderer Bedeutung ist, dass das GeschGehG einheitlich festlegt, was ein Geschäftsgeheimnis ist. Dies ist nach § 2 Nr. 1 jede Information, die

a) weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich ist und daher von wirtschaftlichem Wert ist,
b) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Die Voraussetzungen aus a), b) und c) müssen kumulativ, also nebeneinander vorliegen. Zukünftig erhält demnach nur noch derjenige Know-how-Schutz, der ausreichende Geheimhaltungsmaßnahmen getroffen hat und diese entsprechend belegen kann. Nur dann kann er Ansprüche gegen den Verletzer eines Geschäftsgeheimnisses gerichtlich geltend machen. Leider lässt das Gesetz offen, was unter „angemessenen Geheimhaltungsmaßnahmen“ zu verstehen ist. Die Begründung zum Gesetzentwurf sieht als Geheimhaltungsmaßnahmen grundsätzlich sowohl physische Zugangsbeschränkungen als auch vertragliche Sicherungsmechanismen vor. Da

Geschäftsgeheimnisse vielfach vertrauliche Geschäftsinformationen über Kunden, Personen und Lieferanten enthalten, ist gleichzeitig der parallel im Interesse der Betroffenen bestehende datenschutzrechtliche Schutzauftrag zu erfüllen. Der rbb wird den Anforderungen des GeschGhG - wie auch des Datenschutzes - zukünftig durch sein neues Klassifizierungskonzept für Daten und Informationen (s. C I 1.) Rechnung tragen.

2. Entscheidungen

2.1 Urteile des BVerfG zum „Recht auf Vergessen"

In zwei Entscheidungen hat sich das BVerfG am 06.11.2019 erneut mit der Reichweite des Rechts auf Vergessen in Online-Archiven befasst und damit seine bisherige Rechtsprechung ergänzt und konkretisiert.

Der ersten Entscheidung – 1 BvR 16/13 (Recht auf Vergessen I) lag folgender Sachverhalt zugrunde:

Der Beschwerdeführer wurde im Jahr 1982 rechtskräftig wegen Mordes zu einer lebenslangen Freiheitsstrafe verurteilt, weil er 1981 an Bord einer Yacht auf Hoher See zwei Menschen erschossen hatte. Über den Fall veröffentlichte DER SPIEGEL 1982 und 1983 unter Auseinandersetzung mit der Person des namentlich genannten Beschwerdeführers drei Artikel in seiner gedruckten Ausgabe. Seit 1999 stellt Spiegel Online die Berichte in einem Onlinearchiv kostenlos und ohne Zugangsbarrieren zum Abruf bereit. Gibt man den Namen des Beschwerdeführers in einem gängigen Internetsuchportal ein, werden die Artikel unter den ersten Treffern angezeigt. Nachdem der 2002 aus der Haft entlassene Beschwerdeführer erstmals Kenntnis von der Online-Veröffentlichung erlangt hatte, erhob er nach erfolgloser Abmahnung Unterlassungsklage mit dem Antrag, es der Beklagten zu untersagen, über die Straftat unter Nennung seines Familiennamens zu berichten. Der Bundesgerichtshof (BGH) hatte die Klage abgewiesen. Das BVerfG hat seiner Entscheidung die deutschen Grundrechte als Prüfungsmaßstab zugrunde gelegt, da die in Streit stehende

Verbreitung von Presseberichten unter das sog. Medienprivileg falle, für dessen Ausgestaltung den Mitgliedstaaten unionsrechtlich ein Umsetzungsspielraum zusteht. Auf Seiten des Beschwerdeführers war sein allgemeines Persönlichkeitsrecht (Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 GG) einzustellen. Auf Seiten Spiegel Online hat das BVerfG die Meinungs- und Pressefreiheit (Art. 5 Abs. 1 Satz 1 und 2 GG) herangezogen. Das BVerfG ist der Auffassung, dass unter den heutigen Bedingungen der Informationstechnologie und der Verbreitung von Informationen durch das Internet die Berücksichtigung der Einbindung von Informationen in die Zeit eine neue rechtliche Dimension erhalte. Während Informationen früher als Printmedien und Rundfunksendungen der Öffentlichkeit nur in einem engen zeitlichen Rahmen zugänglich gewesen seien und anschließend weithin in Vergessenheit gerieten, blieben sie heute - einmal digitalisiert und ins Netz gestellt – langfristig verfügbar. Die Informationen könnten jederzeit von völlig unbekannten Dritten aufgegriffen werden, würden Gegenstand der Erörterung im Netz, könnten dekontextualisiert neue Bedeutung erhalten und in Kombination mit weiteren Informationen zu Profilen der Persönlichkeit zusammengeführt werden, wie es insbesondere mittels Suchmaschinen durch Namensbezogene Abfragen verbreitet sei. Bei der Auslegung und Anwendung des allgemeinen Persönlichkeitsrechts sei diesem Umstand Rechnung zu tragen. Allerdings folge aus dem allgemeinen Persönlichkeitsrecht kein „Recht auf Vergessenwerden“ in einem grundsätzlich allein von den Betroffenen beherrschbaren Sinn. Auf der Gegenseite sei nämlich dem Schutzgehalt der Meinungs- und Pressefreiheit angemessen Rechnung zu tragen. Eine Begrenzung auf eine anonymisierte Berichterstattung bedeute eine gewichtige Beschränkung von Informationsmöglichkeiten der Öffentlichkeit sowie des Rechts der Presse, selbst zu entscheiden, worüber sie wann, wie lange und in welcher Form berichtet. Online-Archive ermöglichten einen einfachen Zugang zu Informationen und sind zugleich eine wichtige Quelle für journalistische und zeithistorische Recherchen.

Zusammengefasst gilt nach dem BVerfG folgendes:

Ein Verlag darf anfänglich rechtmäßig veröffentlichte Berichte grundsätzlich auch in ein Onlinearchiv einstellen. Schutzmaßnahmen können erst dann geboten sein, wenn Betroffene sich an ihn gewandt und ihre Schutzbedürftigkeit näher dargelegt haben. Welche Bedeutung verstrichener Zeit für den Schutz gegenüber einer ursprünglich rechtmäßigen Veröffentlichung zukommt, liege maßgeblich in Wirkung und Gegenstand der Berichterstattung, insbesondere darin, wieweit die Berichte das Privatleben und die Entfaltungsmöglichkeiten der Person als ganze beeinträchtigen. Die Belastung der Betroffenen hänge auch daran, wieweit eine Information im Netz tatsächlich breitenwirksam gestreut, etwa wieweit sie von Suchmaschinen prioritär kommuniziert wird.

Für den Ausgleich seinen zudem Abstufungen hinsichtlich der Art möglicher Schutzmaßnahmen seitens des Presseverlags zu berücksichtigen, die die sich ändernden Bedeutungen von Informationen in der Zeit abfedern. Anzustreben sei ein Ausgleich, der einen ungehinderten Zugriff auf den Originaltext möglichst weitgehend erhält, diesen bei Schutzbedarf - insbesondere gegenüber namensbezogenen Suchabfragen mittels Suchmaschinen – aber einzelfallbezogen doch hinreichend begrenzt.

Die angegriffene Entscheidung hält nach Auffassung des BVerfG diesen Anforderungen nicht in jeder Hinsicht stand. Vorliegend sei in Betracht zu ziehen gewesen, ob dem beklagten Presseunternehmen auf die Anzeige des Beschwerdeführers hin zumutbare Vorkehrungen hätten auferlegt werden können und müssen, die zumindest gegen die Auffindbarkeit der Berichte durch Suchmaschinen bei namensbezogenen Suchabfragen einen gewissen Schutz bieten, ohne die Auffindbarkeit und Zugänglichkeit des Berichts im Übrigen übermäßig zu hindern.

In der zweiten Entscheidung (1 BvR 276/17 – Recht auf Vergessen II) wies das BVerfG am selben Tag eine Verfassungsbeschwerde gegen eine Entscheidung des

Oberlandesgerichts (OLG) Celle zurück. In diesem Fall forderte eine Frau vom Suchmaschinenbetreiber Google, die Verknüpfung ihres Namens mit einem Beitrag des Norddeutschen Rundfunks (NDR) aus dem Jahr 2010 aufzuheben. Sie hatte für den Beitrag des Magazins „Panorama" mit dem Titel „Kündigung: Die fiesen Tricks der Arbeitgeber" ein Interview gegeben. Der Beitrag stellte die Kündigung eines damaligen Mitarbeiters eines Unternehmens dar, das sie als Geschäftsführerin leitete. Die Beschwerdeführerin verwahrte sich gegen die Nennung des Begriffs „fiese Tricks" in der Überschrift des Suchergebnisses. Das Suchergebnis rufe eine negative Vorstellung über sie als Person hervor. Sie habe solche Tricks niemals angewandt. In diesem Fall sind nach Angaben der Verfassungsrichter grundsätzlich nicht die deutschen, sondern die Unionsgrundrechte maßgeblich, da die Grundrechte durch den Anwendungsvorrang des Unionsrechts verdrängt werden. Die Grundrechte auf Achtung des Privat- und Familienlebens und der Schutz der personenbezogenen Daten gegen das Recht auf unternehmerische Freiheit des Suchmaschinenbetreibers und das Recht auf Meinungsfreiheit des durch die Entscheidung belasteten NDR sowie das Informationsinteresse der Öffentlichkeit seien abzuwägen. Ein wichtiger Faktor sei auch in diesem Fall die Zeit. Das OLG habe einen Anspruch auf Auslistung zum jetzigen Zeitpunkt noch nicht als gegeben angesehen. Dies sei verfassungsrechtlich nicht zu beanstanden.

2.2 Urteil des BVerwG zur Möglichkeit der Untersagung des Betriebs einer Facebook-Fanpage

Gemäß einem Urteil des Bundesverwaltungsgerichts (BVerwG) vom 11.09.2019 (6 C 15.18) kann der Betreiber einer sog. Fanpage bei Facebook verpflichtet werden, seine Fanpage abzuschalten, falls die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist.

Gegenstand des Revisionsverfahrens war eine Anordnung der schleswig-holsteinischen Datenschutzaufsicht, mit der die Klägerin, eine in Kiel ansässige Bildungseinrichtung, unter der Geltung der Datenschutzrichtlinie (RL 95/46/EG) verpflichtet

worden war, die von ihr bei Facebook betriebene Fanpage zu deaktivieren. In dem Bescheid wurde beanstandet, dass Facebook bei Aufruf der Fanpage auf personenbezogene Daten der Internetnutzer zugreife, ohne dass diese gemäß den Bestimmungen des Telemediengesetzes über Art, Umfang und Zwecke der Erhebung sowie ein Widerspruchsrecht gegen die Erstellung eines Nutzungsprofils für Zwecke der Werbung oder Marktforschung unterrichtet würden. Ein gegenüber der Klägerin als Betreiberin der Fanpage erklärter Widerspruch des Nutzers bleibe mangels entsprechender technischer Einwirkungsmöglichkeiten folgenlos.

Die Klage hatte in den Vorinstanzen noch Erfolg. Das Oberverwaltungsgericht (OVG) hatte eine datenschutzrechtliche Verantwortlichkeit der Klägerin abgelehnt, weil sie keinen Zugriff auf die erhobenen Daten habe. Dagegen wandte sich der Beklagte im vorliegenden Revisionsverfahren. Auf Vorlage des BVerwG hat der EuGH mit Urteil vom 05.06.2018 entschieden, dass der Betreiber einer Fanpage für die durch Facebook erfolgende Datenverarbeitung mitverantwortlich ist. Denn er ermögliche Facebook durch den Betrieb seiner Fanpage den Zugriff auf die Daten der Fanpage-Besucher (15. Tätigkeitsbericht, S. 15).

Das BVerwG hat auf der Grundlage dieser bindenden Vorgabe jetzt das Berufungsurteil aufgehoben und den Rechtsstreit an das schleswig-holsteinische OVG zurückverwiesen. Zur Frage der Rechtswidrigkeit der beanstandeten Datenverarbeitungsvorgänge bedarf es nach Auffassung des BVerwG einer näheren Aufklärung der tatsächlichen Umstände durch das Berufungsgericht. Die Rechtmäßigkeit der bei Aufruf der klägerischen Fanpage ablaufenden Datenverarbeitungsvorgänge sei an den Vorgaben des im Zeitpunkt der letzten Behördenentscheidung gültigen Datenschutzrechts, insbesondere an den Vorschriften des Telemediengesetzes, denen die Klägerin als Betreiberin unterliege, zu messen.

Um das von der Datenschutzrichtlinie bezweckte hohe Datenschutzniveau möglichst zügig und wirkungsvoll durchzusetzen, habe sich der Beklagte bei der Auswahl unter

mehreren datenschutzrechtlichen Verantwortlichen vom Gedanken der Effektivität leiten lassen und ermessenfehlerfrei die Klägerin für die Herstellung datenschutzkonformer Zustände bei Nutzung ihrer Fanpage in die Pflicht nehmen können. Er habe nicht gegen eine der Untergliederungen oder Niederlassungen von Facebook vorgehen müssen, weil das wegen der fehlenden Kooperationsbereitschaft von Facebook mit erheblichen tatsächlichen und rechtlichen Unsicherheiten verbunden gewesen wäre. Würden sich die bei Aufruf der Fanpage ablaufenden Datenverarbeitungen als rechtswidrig erweisen, so stelle die Deaktivierungsanordnung ein verhältnismäßiges Mittel dar, weil der Klägerin keine anderweitige Möglichkeit zur Herstellung datenschutzkonformer Zustände offenstehe.
Die Entscheidung des schleswig-holsteinischen OVG bleibt abzuwarten.

2.3 Urteil des BVerwG zur Härtefallbefreiung

Unter Aufgabe seiner bisherigen Rechtsprechung hat das BVerwG mit Urteil vom 30.10.2019 entschieden, dass ein besonderer Härtefall gemäß § 4 Abs. 6 Satz 1 Rundfunkbeitragsstaatsvertrag (RBStV) vorliegt, wenn das monatlich für den Lebensbedarf zur Verfügung stehende Einkommen von Beitragsschuldnern, die keine Leistungen im Sinne von § 4 Abs. 1 RBStV erhalten und über kein verwertbares Vermögen verfügen, nach Abzug der Wohnkosten unterhalb des für den Bezug von Hilfe zum Lebensunterhalt maßgebenden Regelsatzes liegt (BVerwG 6 C 10.18). In diesem Fall bestehe ein Anspruch auf Befreiung von der Rundfunkbeitragspflicht.

Dieses Urteil hat eine Studentin erstritten, die wegen Studienfachwechsel keine BaföG-Leistungen mehr erhält und gegenüber dem zuständigen Bayerischen Rundfunk (BR) nachgewiesen hatte, dass ihr Einkommen nach Abzug der Wohnkosten mit dem Einkommen der Empfänger von Sozialleistungen nach dem SGB XII vergleichbar und kein verwertbares Vermögen vorhanden ist.

Bislang haben die Rundfunkanstalten einen besonderen Härtefall mit Verweis auf die Rechtsprechung des BVerwG in Fällen, in denen die beitragspflichtige Person – wie

hier - zwar dem Grunde nach von den Fallgestaltungen des Absatzes 1 erfasst wird, sie aber deren Voraussetzungen nicht bzw. nicht vollständig erfüllt, verneint. Ein Antrag auf Befreiung nach § 4 Abs. 6 S.1 RBStV, der allein auf den Fakt eines geringen Einkommens gestützt war, wurde stets abgelehnt. Es bestand lediglich eine bescheidgebundene Befreiungsmöglichkeit. Diese Praxis entsprach auch der Intention des Gesetzgebers, der mit der Neuregelung von § 6 Abs. 3 Rundfunkgebührenstaatsvertrag (RGebStV) (Vorgängerregelung zu § 4 Abs. 6 RBStV) die zuvor rechtlich gebotene aufwändige Berechnung des geringen Einkommens für die Frage der Rundfunkgebührenpflicht abgeschafft hatte.

Das BVerwG hat seine zu § 6 Abs. 3 RGebStV ergangene Rechtsprechung nun unter Verweis auf den Schutz des Existenzminimums aufgegeben. Während die nach § 4 Abs. 1 Nr. 1 RBStV von der Rundfunkbeitragspflicht befreiten Personen nicht auf das monatlich ihnen zur Verfügung stehende Einkommen in Höhe der Regelleistungen zur Erfüllung der Beitragspflicht zurückgreifen müssen, weil dieses Einkommen ausschließlich zur Deckung ihres Lebensbedarfs einzusetzen ist, müssten Personen wie die Klägerin auf ihr der Höhe nach den Regelleistungen entsprechendes oder diese Höhe sogar unterschreitendes Einkommen zurückgreifen, weil sie aus dem System der Befreiung nach § 4 Abs. 1 RBStV herausfallen. Sie würden dadurch schlechter gestellt, obwohl beide Personengruppen in Bezug auf ihre finanzielle Bedürftigkeit miteinander vergleichbar seien. Eine solche Ungleichbehandlung beruhe nicht auf einem sachlichen Grund.

Nach dem Urteil müssen die Rundfunkanstalten bzw. der Zentrale Beitragsservice (ZBS) nun in vergleichbaren Fällen eine aufwändige Bedürftigkeitsprüfung durchführen. Hierfür müssen die Beitragsschuldner ihnen die erforderlichen Nachweise vorlegen. Erfüllen Antragsteller die ihnen rechtmäßig auferlegten Mitwirkungspflichten trotz angemessener Fristsetzung nicht, ist die Befreiung zu versagen. Der ZBS muss nun ein neues Verfahren für eine solche Bedürftigkeitsprüfung aufsetzen. Da in diesem Zusammenhang in großem Umfang sensible personenbezogene Daten

verarbeitet werden, muss das neue Verfahren mit den Datenschutzbeauftragten der Rundfunkanstalten abgestimmt werden.

III. Berlin/Brandenburg

1. Normen

1.1 22. Rundfunkänderungsstaatsvertrag

Am 01.05.2019 ist der 22. Rundfunkänderungsstaatsvertrag (RÄndStV) in Kraft getreten. Er hat vor allem die zeitgemäße Ausweitung des Telemedienauftrags des öffentlich-rechtlichen Rundfunks zum Gegenstand. Die Kernpunkte der Novellierung betreffen die Herstellung eigenständiger audiovisueller Inhalte für die Online-Verbreitung, das Angebot der Inhalte auch außerhalb des dafür jeweils eingerichteten Portals, die Neuregelung zur Feststellung presseähnlicher Telemedien sowie die Erweiterung des inhaltlichen Umfangs von Telemedienkonzepten. Die Gestaltung der Telemedienangebote soll die Belange der Menschen mit Behinderungen besonders berücksichtigen.

1.2 23. Rundfunkänderungsstaatsvertrag

Am 01.06.2020 wird der 23. RÄndStV in Kraft treten. Er wurde auf der Ministerpräsidentenkonferenz im Oktober 2019 unterzeichnet. Schwerpunkte des 23. RÄndStV sind zum einen die Umsetzung der Vorgaben des BVerfGs zur Befreiung von der Rundfunkbeitragspflicht für Zweitwohnungsinhaber*innen und zum anderen die Einführung eines regelmäßigen alle vier Jahre stattfindenden Meldedatenabgleichs – beginnend ab dem Jahr 2022. Bezüglich der personenbezogenen Daten ist dabei eine klare Zweckbindung gegeben und nicht erforderliche Daten werden unverzüglich gelöscht. Der regelmäßige Meldedatenabgleich soll dann nicht durchgeführt werden, wenn die Kommission zur Ermittlung des Finanzbedarfs (KEF) im Rahmen ihres Berichts feststellt, dass der Datenbestand der Landesrundfunkanstalten hinreichend aktuell ist. Mit diesem Instrument soll die Verhältnismäßigkeit zwischen

Beitragsgerechtigkeit und dem Recht auf informationelle Selbstbestimmung gewahrt werden. Die weiteren Anpassungen sind Folgeänderungen aufgrund der DSGVO. Unter anderem wird der Umfang des datenschutzrechtlichen Auskunftsanspruchs in einer Art und Weise, die den Anforderungen des Art. 23 DSGVO gerecht wird, konkretisiert.

In der am 29.04.2019 stattgefundenen nichtöffentlichen mündlichen Anhörung der Länder hat die rbb-Datenschutzbeauftragte gemeinsam mit dem Vorsitzenden des Arbeitskreises der Datenschutzbeauftragten des öffentlich-rechtlichen Rundfunks (AK DSB), Herrn Dr. Heiko Neuhoff, die Positionen des AK DSB zu dem Entwurf vorgetragen. Danach handelt es sich bei dem vorgesehenen regelmäßigen Meldedatenabgleich nicht um eine unzulässige Vorratsdatenspeicherung. Er ist zur angestrebten Vermeidung eines Vollzugsdefizits und Herstellung größerer Beitragsgerechtigkeit geeignet und verhältnismäßig.

1.3 Entwurf des neuen Medienstaatsvertrags

Der Rundfunkstaatsvertrag gilt bisher nur für ausgewählte Medienformen, wie Telemedien oder Plattformen und regelt den privaten und öffentlichen Rundfunk ausführlich. Am 05.12.2019 haben die Ministerpräsidenten einen Beschluss zu dem Entwurf für einen neuen Medienstaatsvertrag gefasst. Danach sollen auch für Online-Anbieter wie Google und Facebook künftig wichtige Grundsätze des Medienrechts gelten. Um den neuen Regelungsinhalt auch nach außen zu verdeutlichen, wird der Rundfunkstaatsvertrag in Medienstaatsvertrag umbenannt. Reformiert werden soll unter anderem die Zulassungspflicht für Rundfunkangebote. Bisher gab es immer wieder Ärger, weil zum Beispiel Youtuber mit mehr als 500 gleichzeitigen Zuschauern für ihre Live-Videos Lizenzen brauchten. Künftig sollen solche Anbieter keine Zulassung benötigen, wenn sie im Durchschnitt weniger als 20.000 gleichzeitige Nutzer erreichen oder nur eine geringe Bedeutung für die individuellen und öffentliche Meinungsbildung entfalten. Ferner wird der Begriff „Medienintermediäre“ eingeführt. In diese Sparte fallen Plattformen wie Google und Facebook. Aber auch für

Sprachassistenten und smarte Lautsprecher wie „Alexa“ sollen künftig die Regelungen des Staatsvertrages gelten.

1.4 Entwurf eines Ersten Medienänderungsstaatsvertrags

Auf Vorlage des Regierenden Bürgermeisters hat der Berliner Senat am 31.03.2020 dem Entwurf des Ersten Medienänderungsstaatsvertrages zugestimmt und ihn zur Unterzeichnung nach Unterrichtung des Abgeordnetenhauses ermächtigt. Inhalt des Ersten Medienänderungsstaatsvertrages ist zum einen die Umsetzung der von der KEF in ihrem 22. KEF-Bericht ausgesprochenen Empfehlung, den Rundfunkbeitrag in der nächsten Beitragsperiode (Zeitraum 2021 bis 2024) von derzeit 17,50 € auf dann 18,36 € zu erhöhen. Zum anderen wird eine Anpassung des zugunsten von RB und des Saarländischen Rundfunks (SR) bestehenden ARD-Finanzausgleichs durch schrittweise Anhebung der Finanzausgleichsmasse vorgenommen. Mit der Beitragsanpassung wird an die Rundfunkanstalten die Erwartung geknüpft, ihre bisherigen Reformbemühungen fortzusetzen und weitere, über reine Rationalisierungsprozesse hinausgehende Einsparungen zu erzielen.

2. Entscheidungen

2.1 Beschluss des OVG Berlin-Brandenburg zum Umfang des Informationsanspruchs der rbb-Freienvertretung

Mit Beschluss vom 19.12.2019 hat das OVG Berlin-Brandenburg einen Antrag der Freienvertretung auf regelmäßige Überlassung von umfangreichen Informationen über arbeitnehmerähnliche Personen im rbb zurückgewiesen. Dem Beschluss lag folgender Sachverhalt zugrunde:

Zur Erfüllung ihrer Aufgaben übermittelt die HA Personal der Freienvertretung regelmäßig auf der Grundlage von § 36 Freienstatut (FS) verschiedene anonymisierte Listen mit Angaben zu den beim rbb beschäftigten arbeitnehmerähnlichen Personen. Nach Auffassung der Freienvertretung benötigt sie weitere Informationen zur Erfüllung ihrer Aufgaben nach dem FS. Mit Schreiben vom 15.04.2016 forderte sie eine

pseudonymisierte Liste sowie gesondert eine namentliche Liste – jeweils mit zahlreichen Einzelangaben - an. Diese Forderung lehnte die HA Personal – gestützt auf ein Votum der rbb-Datenschutzbeauftragten - ab, da über die bereits erteilten regelmäßigen Informationen hinaus kein Anspruch auf weitere Datenübermittlung bestehe. Außerdem seien einige erbetene Informationen technisch nicht zu ermitteln. Am 06.04.2017 hat die Freienvertretung daraufhin beim Verwaltungsgericht (VG) Berlin den Antrag gestellt festzustellen, dass der rbb verpflichtet ist, ihr quartalsweise 1. eine pseudonymisierte Liste sowie 2. eine namentliche Liste jeweils mit genau genannten Daten (u. a. Merkmale besonderer Schutzbedürftigkeit wie Schwerbehinderung, chronische Krankheiten, Schwangerschaft) arbeitnehmerähnlicher Mitarbeiterinnen und Mitarbeiter zur Verfügung zu stellen. Mit Beschluss vom 03.07.2019 hat das VG Berlin den Antrag zurückgewiesen. Dagegen hat die Freienvertretung beim OVG Berlin-Brandenburg teilweise Zulassung der Berufung beantragt. Nach mündlicher Verhandlung am 19.12.2019, an der die Datenschutzbeauftragte als Prozessbeobachterin teilgenommen hat, hat das OVG die Beschwerde zurückgewiesen. Die Freienvertretung begehre mit der pseudonymisierten Liste über sämtliche arbeitnehmerähnliche Mitarbeiterinnen und Mitarbeiter gleichsam einen Steckbrief jeder einzelnen Person ohne Namensnennung. Von einem solchen Anspruch sei in § 36 Abs. 2 Nr. 1 FS nicht die Rede. Das FS mache eine über § 36 Abs. 2 Nr. 1 hinausgehende, intensivere, insbesondere personenbezogene Information über den in Nr. 1 geregelten Lebenssachverhalt zum Sonderfall. Die Anmeldung eines weitergehenden Informationsbedarfs, eines Sonderfalls, setze voraus, dass die Freienvertretung einen bestimmten Prüfanlass nenne. Diesen habe sie zwar hier geltend gemacht, indem sie anhand der ihr bereits vorliegenden Informationen auf eine durchschnittlich geringere Honorierung von Frauen bei annähernd derselben Arbeitszeit wie Männer verweise. Dieser angeführte Sonderfall verpflichte indes die Beteiligte nicht zur halbjährlichen Herstellung und Überlassung von Listen mit dem beantragten Inhalt. Gemessen an dem von der Antragstellerin benannten Anlass, auf die Förderung der finanziellen Gleichberechtigung von Frauen und Männern hinzuwirken, seien die von ihr angeforderten Unterlagen nicht „erforderlich“ im Sinne von § 36 Abs. 1 FS. Ob Unterlagen erforderlich sind, ergebe sich in der Abwägung von Informations- und

Datenschutzbelangen. Diese gehe zum Nachteil der Freienvertretung aus. Nach Art. 6 Abs. 1 Satz 1 Buchstabe e) DSGVO sei die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Es erschließe sich für den Senat nicht, warum die Fülle der angeforderten Informationen, die mehr als nur im Einzelfall den Rückschluss auf die natürliche Person erlaube, zur Aufklärung des Anlasses benötigt wird. Dies betreffe insbesondere die Krankheitsdaten, die gemäß Art. 36 Abs. 1 des rbb-StV i. V. m. § 14 BlnDSG nur unter besonderen Voraussetzungen erlaubt sei. Es liege auf der Hand, das die Fülle der Informationen in den Steckbriefen den Rückschluss auf die natürliche Person erheblich erleichtert und dass gerade auch in ihrer Sinnhaftigkeit für den Prüfanlass zweifelhafte Informationen wie etwa die Zahl der Kinder oder eine spezifische Schutzbedürftigkeit aufgrund vorhandenen Wissens bei Mitgliedern der Freienvertretung den Rückschluss auf bestimmte Personen und das von ihnen erzielte Gehalt erlauben. Gesundheitsdaten in den Steckbriefen wären einer natürlichen Person zuzuordnen. Das gehe weit über das hinaus, was für die Aufklärung der Ursachen für anscheinend vorhandene Unterschiede der Honorierung notwendig und angemessen ist. Wegen grundsätzlicher Bedeutung hatte das OVG Rechtsbeschwerde gegen den Beschluss zugelassen. Nachdem die Freienvertretung von dieser Möglichkeit keinen Gebrauch gemacht haben, ist der Beschluss rechtskräftig.

2.2 Bußgeldbescheid der Berliner Datenschutzbeauftragte gegen die Deutsche Wohnen SE

Am 30.10.2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro wegen Verstößen gegen die DSGVO erlassen.

Bei Vor-Ort-Prüfungen im Juni 2017 und im März 2019 hatte die Aufsichtsbehörde festgestellt, dass das Unternehmen für die Speicherung personenbezogener Daten

von Mieter*innen ein Archivsystem verwendete, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen. Personenbezogene Daten der Mieter*innen wurden gespeichert, ohne zu überprüfen, ob eine Speicherung zulässig oder überhaupt erforderlich ist. In begutachteten Einzelfällen konnten daher teilweise Jahre alte private Angaben betroffener Mieter*innen eingesehen werden, ohne dass diese noch dem Zweck ihrer ursprünglichen Erhebung dienten. Es handelte sich dabei um Daten zu den persönlichen und finanziellen Verhältnissen, wie z. B. Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge. Nachdem die Berliner Datenschutzbeauftragte im ersten Prüftermin 2017 die dringende Empfehlung ausgesprochen hatte, das Archivsystem umzustellen, konnte das Unternehmen auch im März 2019, mehr als eineinhalb Jahre nach dem ersten Prüftermin und neun Monate nach Wirksamwerden der DSGO, weder eine Bereinigung ihres Datenbestandes noch rechtliche Gründe für die fortdauernde Speicherung vorweisen. Zwar hatte das Unternehmen Vorbereitungen zur Beseitigung der aufgefundenen Missstände getroffen. Diese Maßnahmen hatten jedoch nicht zur Herstellung eines rechtmäßigen Zustands bei der Speicherung personenbezogener Daten geführt.

Die Sanktion gegenüber der Deutschen Wohnen SE führt deutlich vor Augen, wie gravierend ein mangelndes bzw. mangelhaftes Löschkonzept von der Aufsichtsbehörde bewertet wird. Die Erarbeitung angemessener Löschkonzepte ist daher ein zentraler Bestandteil des neuen Datenschutzmanagements beim rbb.

C. Datenschutz und Datensicherheit im rbb

I. Neue Regelwerke

1. Dienstanweisung Informationsmanagement

Wie im letzten Tätigkeitsbericht (15. Tätigkeitsbericht, S. 28 ff.) erwähnt, hatte die Geschäftsleitung am 24.04.2019 auf Vorschlag des „Projekts zur Umsetzung der DSGVO“ beschlossen, die alte Datenschutz-Dienstanweisung aus dem Jahr 2005 durch eine zeitgemäße und DSGVO-konforme Anweisung zu ersetzen und auch die Dienstanweisung Auftragsdatenverarbeitung an die DSGVO anzupassen. Die beiden geänderten Dienstanweisungen gelten seit ihrer Veröffentlichung am 10.05.2019. Seitdem haben u. a. Veränderungen in der eingesetzten Hard- und Software und das verstärkte mobile Arbeiten weitere Überarbeitungen des rbb-internen Regelungswerkes erforderlich gemacht. Gemeinsam mit den Kollegen aus der Informationssicherheit habe ich daher den Entwurf für eine Dienstanweisung Informationsmanagement mit elf Anlagen erarbeitet. Darin werden nun sämtliche rbb-internen Anforderungen an die Verarbeitung von Daten und Informationen insgesamt neu geordnet und in einer einheitlichen Dienstanweisung zusammengefasst. Gleichzeitig werden das Auffinden und die Aktualisierung von konkreten Handlungsanweisungen durch die Verschiebung in die jeweiligen Anlagen erleichtert. Neu ist unter anderem ein Klassifizierungskonzept für Daten und Informationen. Danach müssen die Nutzer*innen für jedes Dokument eine Schutzklasse auswählen. An die Schutzklasse knüpfen jeweils entsprechende technische und organisatorische Maßnahmen an. Die Dienstanweisung Informationsmanagement wird folgende bisher bestehenden Dienstanweisungen ersetzten:

- Datenschutz-Dienstanweisung vom 06.05.2019,
- Dienstanweisung Auftragsverarbeitung vom 06.05.2019,
- Dienstanweisung IT-Nutzung vom 24.08.2017,

- Dienstanweisung zur Gewährleistung der Informationssicherheit vom 23.04.2014 und
- Dienstanweisung für die Bearbeitung und Verwaltung von Dokumenten und Akten vom 29.03.2011.

Wir haben den Entwurf mit dem Kreis der Datenschutz-Koordinatoren (s. II 1.) und den Mitgliedern des IT-Sicherheitskreises (s. II 2.) abgestimmt. Die Mitarbeitervertretungen waren ebenfalls an dem Abstimmungsprozess beteiligt und haben den Entwurf aktiv zur Kenntnis genommen. Zum Zeitpunkt des Redaktionsschlusses dieses Tätigkeitsberichts dauerte die Befassung der Geschäftsleitung mit dem Entwurf der neuen Dienstanweisung noch an.

II. Arbeitsgruppen und übergeordnete Projekte

1. Datenschutz-Koordinatoren

Das Datenschutz-Management des rbb sieht sog. Datenschutz-Koordinatoren vor. Danach benennt jede Direktion einen Datenschutz-Koordinator/ eine Datenschutz-Koordinatorin. Zusätzlich haben auch die Intendanz und das Justitiariat einen Datenschutz-Koordinator bzw. eine Datenschutz-Koordinatorin benannt.

Die Datenschutz-Koordinatoren stellen das Bindeglied zwischen der Datenschutzbeauftragten und der jeweiligen Direktion dar. Konkret fallen den Datenschutzkoordinatoren folgende Aufgaben zu:

- Vermittlung von datenschutzrechtlichen Vorgaben in die Direktion bzw. in die Intendanz und das Justitiariat,

- frühzeitige Information der Datenschutzbeauftragten über datenschutzrechtlich relevante Vorhaben und Projekte aus der Direktion bzw. aus der Intendanz und dem Justitiariat,

- Unterstützung der Datenschutzbeauftragten bei der Organisation von Datenschutzunterweisungen,

- Unterstützung der Informationsverantwortlichen bei Meldungen zum Verzeichnis von Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DSGVO,

- Unterstützung der Informationsverantwortlichen bei der Formulierung von Datenschutz-Informationen gemäß Art. 13. und 14 DSGVO und

- Unterstützung der Datenschutzbeauftragten bei dem Entwurf von konkreten und praktikablen datenschutzrechtlichen Vorgaben im rbb.

An den Treffen der Datenschutz-Koordinatoren nehmen neben der Datenschutzbeauftragten, ihrem Stellvertreter und ihrem Mitarbeiter die Datenschutz-Koordinatoren sowie der Informationssicherheitsbeauftragte und dessen Stellvertreter teil. Je nach Bedarf und Thema werden auch die Mitarbeitervertretungen einbezogen.

Am 24.10.2019 fand das erste Datenschutz-Koordinatoren-Treffen statt. Themen waren das neue Datenschutz-Management im rbb, insbesondere die Rolle der Datenschutz-Koordinatoren. Außerdem wurden diverse Einzelfragen besprochen und Verabredungen zur Arbeitsweise des Kreises der Datenschutz-Koordinatoren getroffen. In den Sitzungen am 21.11.2019 und am 09.01.20 hat sich das Gremium monothematisch mit dem Entwurf der neuen Dienstanweisung Informationsmanagement befasst. In der gemeinsamen Sitzung mit dem Informationssicherheitskreis am 10.03.2020 wurde der Entwurf der Dienstanweisung Informationsmanagement abschließend behandelt.

2. Informationssicherheitskreis

Der vom Informationssicherheitsbeauftragten geleitete Informationssicherheitskreis, dem auch die Datenschutzbeauftragte angehört, tagte im Berichtszeitraum am 29.04. und 18.11.2019 sowie am 10.03.2020. Am 29.04.2019 hat sich der Kreis mit dem Stand des Projekts „Sicherheitskonzept rbb" (s. dazu III. 4.), mit dem Sicherheitskonzept für MS Office 365 und mit einzelnen Sicherheitsvorfällen im rbb beschäftigt. Schwerpunktthemen der Sitzung am 18.11.2019 waren u. a. die Konfiguration mobiler Endgeräte, die geplante Datenklassifizierung, der Stand des Projekts „MS Office 365" (s. III 1.) sowie der Entwurf einer neuen Passwortrichtlinie. In der gemeinsamen Sitzung mit dem Kreis der Datenschutz-Koordinatoren am 10.03.2020 wurde der Entwurf der Dienstanweisung Informationsmanagement abschließend behandelt.

3. Jour Fixe IT-Projekte

In regelmäßigen Terminen hatte die damalige Bereichsleiterin „Projekte und Organisation" der ehemaligen Abteilung Organisation und IT (OUI) in der Vergangenheit die Mitglieder des Personalrats, die Schwerbehindertenvertretung und die Datenschutzbeauftragte in einem informellen Rahmen über geplante und laufende Projekte informiert. Dieser Rahmen ermöglichte es, offen über Ideen und Probleme zu reden und Beteiligungsrechte zu einem möglichst frühen Zeitpunkt zu identifizieren. Im Berichtszeitraum fand ein Termin am 17.06.2019 statt. An dem Termin hat der stellvertretende Datenschutzbeauftragte teilgenommen. Es ging um nachfolgende Themen:

- Einführung von MS Office 365 (s. III 1.),
- „print at work" – Druckermanagementsystem im rbb (s. C III 8.) und
- geplanter gemeinsamer Zentraler Service Desk in der ARD.

Die Abteilung OUI existiert nach der Neuorganisation der Hauptabteilung Mediensysteme und IT (MIT) in seiner ursprünglichen Form nicht mehr. Ob es eine Fortsetzung des Jour Fixe IT-Projekte gibt, ist nicht bekannt. Aus Sicht der Datenschutzbeauftragten wäre dies wünschenswert.

4. Restarbeiten aus dem Projekt zur Umsetzung der DSGVO

Im Rahmen des Projekts zur Umsetzung der DSGVO, dessen Laufzeit im Frühjahr 2019 beendet war (s. 15. Tätigkeitsbericht S. 35 ff.), konnten nicht alle Bereiche im rbb individuell angesprochen werden. Da eine individuelle Ansprache gerade bei grundlegenden Veränderungen sehr wichtig ist, wurden seitens der Datenschutzbeauftragten nach dem Projektende die entsprechenden Informationsmaßnahmen weitergeführt. In diesem Zusammenhang sind die folgenden Informationsveranstaltungen/Gespräche zu erwähnen:

- Informationsveranstaltung für Schwerbehindertenvertretung, Frauenbeauftragte und Suchtbeauftragten am 05.04.2019
- Informationsveranstaltung HA Personal am 03.05.2019
- Gespräch mit Konfliktmanagerin am 13.05.2019
- Informationsveranstaltung HA Medienproduktion 14.06.2019
- Informationsveranstaltung Qualitätsmanagement und Medienforschung am 22.08. 2019
- Gespräch mit Sendeleitung Fernsehen 25.09.2019
- Gespräch mit On-Air Design und Präsentation 25.09.2019
- Gespräch mit Online Koordination 25.09.2019
- Gespräch mit Programmbegleitende Dienste 23.10.2019
- Gespräch mit Antenne Brandenburg 23.10.2019
- Gespräch mit Programmplanung 23.10.2019
- Gespräch mit HA Programm-Management 26.11.2019
- Gespräch mit zibb / Super.Markt 26.11.2019
- Gespräch mit Programmkoordination 05.12.2019

- Gespräch mit Herstellungs- und Etatmanagement 05.12.2019
- Gespräch mit Radio Fritz 17.01.2020
- Gespräch mit radioeins 17.01.2020

In diesen Terminen wurde jeweils individuell zum Datenschutz bei der Büroorganisation (u. a. Dienstplangestaltung und Dienstreiseplanung) und bei der Durchführung der spezifischen Aufgaben der jeweiligen Bereiche nach Maßgabe der DSGVO beraten. Diese spezifischen Informationsveranstaltungen werden im neuen Berichtsjahr fortgesetzt.

III. IT-Projekte

1. MS Office 365

1.1 Stand des Projektes

Wie berichtet (zuletzt 15. Tätigkeitsbericht, S. 40 ff.) hat der rbb die Entscheidung getroffen, zur besseren Unterstützung seiner Geschäftsprozesse die zentralen Microsoft Office-Anwendungen auf die cloudbasierte Lösung Office 365 zu migrieren. Zu den grundsätzlichen Zweifeln an der DSGVO-Konformität der Microsoft-Cloud habe ich mich in meinen früheren Tätigkeitsberichten (zuletzt 15. Tätigkeitsbericht, S. 40 ff.) geäußert. Die Zweifel konnte Microsoft bis heute nicht vollends ausräumen. Problematisch ist, dass Microsoft neben den Funktions- und Inhaltsdaten bei der Bereitstellung von Office 365 eine Vielzahl sog. Diagnosedaten verarbeitet. Diese Daten werden für die Nutzung verschiedener Funktionalitäten wie die Rechtschreibprüfung, Übersetzungen und Office Hilfe benötigt. Microsoft behält sich bei 14 verschiedenen Arten dieser Diagnosedaten eine Nutzung auch zu eigenen Zwecken (Qualitätsverbesserung) vor. Allerdings bietet Office 365 mittlerweile die Option an, die Übertragung dieser Daten zu deaktivieren. Der rbb hat die Übertragung der Diagnosedaten überall dort deaktiviert, wo es für den rbb nicht zu größeren Einbußen in der Nutzbarkeit führt.

Bereits am 15.09.2017 hat der rbb einen Probebetrieb mit Fokussierung auf die Applikationen SharePoint, OneDrive für Business und das Office pro Plus-Paket (Word, Excel, PowerPoint, OneNote etc.) gestartet, an dem die ehemalige Abteilung OUI (jetzt HA MIT) und die gesamte Geschäftsleitung sowie weitere Bereiche des rbb teilnehmen. Der Probebetrieb war ursprünglich bis August 2018 befristet und wurde zunächst bis Ende Februar 2019 verlängert. Es folgte eine weitere Verlängerung und Ausweitung des Probebetriebs auf das Mail-System Outlook und Exchange. Unterdessen hat die Geschäftsleitung entschieden, sich zunächst auf Outlook als neues Programm für Mails, Kalender und Kontakte zu fokussieren. Am Ende des ersten Quartals 2020 waren im Wesentlichen alle rbb-Mitarbeiter auf Outlook migriert.

Wie berichtet hatte die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (PWC) im Auftrag der Datenschutzbeauftragten im Februar 2019 die bis dahin vorgelegten Planungskonzepte der HA MIT bewertet. PWC war seinerzeit zu dem Ergebnis gekommen, dass die Gewährleistung des Datenschutzes in den Konzepten noch nicht mit der notwendigen Präzision geplant worden war. Besonders kritisch wurde von PWC das Vorhaben eingeschätzt, den rbb-Mitarbeiter*innen und Dritten Vollzugriff auf die rbb-Cloud mit rbb-fremden Geräten zu gewähren. Mit den ursprünglich zum Erwerb geplanten Lizenzen hätte im Falle einer Kompromittierung dieser Geräte durch Schadsoftware eine unerlaubte Weitergabe personenbezogener Daten durch den rbb weder erkannt noch verhindert werden können. Diesen Lizenzen fehlen wesentliche Leistungsmerkmale zur Steuerung und Überwachung von Zugriffen auf sensible Daten seitens des rbb. Ihre Zustimmung zur Verlängerung des Probebetriebs hatte die Datenschutzbeauftragte daher davon abhängig gemacht, dass das ursprüngliche Datenschutzkonzept überarbeitet und um Feinkonzepte erweitert wird. Dies schloss den Erwerb Lizenzen mit zusätzlichen Schutzfunktionen ein. Auf ihrer Sitzung am 31.07.2019 hat die Geschäftsleitung nach Anhörung der Datenschutzbeauftragten beschlossen, den notwendigen Schutz für Office 365 durch zusätzliche technische und organisatorische Maßnahmen (insbesondere durch Beschaffung der zusätzlichen Schutz bietenden Lizenzen) zu realisieren. Gleichzeitig

hat sie entschieden, allen festen und freien Mitarbeiter*innen die Nutzung von Office 365 auch mit privaten Endgeräten zu gestatten.

Während MS Office 365 im rbb verteilt wurde, hat die Datenschutzbeauftragte gemeinsam mit dem Informationssicherheitsbeauftragten und der Projektleitung Handlungsanweisungen und Tipps für die Nutzer*innen zur individuellen Erhöhung des Datenschutzes beim Gebrauch von MS Office 365 erarbeitet. Außerdem war sie an der Erstellung der endgültigen Fassung des Sicherheitskonzepts beteiligt und hat das Betriebs-, das Berechtigungs- und das Supportkonzept geprüft. Darüber hinaus hat sie die Projektleitung beim Ausfüllen des VVT-Erfassungsbogens und bei der Formulierung der Nutzungsbedingen unterstützt. Schließlich hat sie an der finalen Fassung des Entwurfs für die Dienstvereinbarung zu Office 365 mitgearbeitet. Dabei wurden die von der RDSK in einem Eckpunkte-Papier für den Einsatz cloudbasierter Office-Systeme definierten Anforderungen berücksichtigt (s. dazu Anlage 2). Nachdem die Dokumentenlage vollständig und den Anforderungen des Datenschutzes weitestgehend Rechnung getragen worden war, konnte die Datenschutzbeauftragte dem Regelbetrieb von Office 365 zustimmen.

Schneller als ursprünglich geplant, wurden im März 2020 während einer urlaubsbedingten Abwesenheit der Datenschutzbeauftragten mit Zustimmung ihres Stellvertreters die Systemkomponenten Teams und OneDrive „ausgerollt“ (=verteilt). Hintergrund war die Corona-bedingte Notwendigkeit des virtuellen Zusammenarbeitens. Teams bietet eine Möglichkeit für die vernetzte Zusammenarbeit in Teams und Projekten mit Dokumentenablage, Chat sowie (Video-)Anruf und Besprechungsfunktionen. OneDrive ist der zentrale, persönliche Speicherort für die Daten der Beschäftigten in Office 365 und ergänzt das bislang zur Verfügung stehende H-Laufwerk. Die Nutzung von Teams bedeutet nach Einschätzung der Datenschutzbeauftragten einen echten Gewinn für die tägliche Arbeit. Den spezifischen datenschutzrechtlichen Problempunkten konnte mit entsprechenden Empfehlungen zur Nutzung im Hinweispapier zum Datenschutz für die Nutzer*innen begegnet werden.

1.2 Schulungsplattform für MS Office 365

Im Sommer 2019 hat der rbb seinen Mitarbeiter*innen eine Lernplattform zur Verfügung gestellt, mit deren Hilfe sie sich Kenntnisse im Umgang mit der neuen Bürosoftware MS Office 365 aneignen können. Anbieter dieser Plattform ist ein Stuttgarter Unternehmen, das bereits beim SWR ein ähnliches Angebot erfolgreich etabliert hat. Die Plattform wurde an das rbb-Intranet angebunden. Die Nutzer können über das Intranet in die Lernumgebung des Anbieters wechseln. Auf der Plattform gibt es Texte und Videos, in denen die einzelnen Anwendungen von MS Office 365 erklärt werden. Zur Authentifizierung als Mitarbeiter*in des rbb übermittelt der rbb beim Klick auf den Link im Intranet einen zufallsgenerierten sog. Globally Unique Identifier (GUID). Dieser GUID dient außerdem zur Registrierung, an welcher Stelle ein Nutzer bzw. eine Nutzerin ein Lehrvideo stoppt; anhand dieser Information kann der Nutzer/die Nutzerin zu einer späteren Zeit wieder am gleichen Punkt in das Video einsteigen. Außerdem können sich die Nutzer*innen persönliche Favoriten markieren. Der GUID ist kein personenbezogenes Datum. Selbst im Falle eines kollusiven Zusammenwirkens der Administratoren im rbb und der Anbieterfirma wäre die Möglichkeit einer Zuordnung des GUID zu einer konkreten Person im rbb ausgeschlossen, da der GUID beim Anbieter verschlüsselt wird. Die Datenschutzbeauftragte hatte keine datenschutzrechtlichen Einwände gegen den Einsatz der Schulungsplattform beim rbb.

2. Mobiles Arbeiten im Homeoffice während der Corona-Pandemie

Anfang März 2020 haben die Corona-Pandemie und die in diesem Zusammenhang getroffenen Regierungsanordnungen zur Beschränkung der sozialen Kontakte auch im rbb zu massiven Änderungen der Arbeitsweise geführt. Alle nicht senderelevanten Mitarbeiter*innen wurden ins Homeoffice geschickt. In dieser Situation war und ist es ein großer Vorteil, dass der rbb mit der Einführung von MS Office 365 bereits die Möglichkeiten des mobilen Arbeitens vorbereitet hatte. In gebotener Eile wurde mit Zustimmung des stellvertretenden Datenschutzbeauftragten die Einführung der Applikationen Teams und OneDrive vorgezogen (s. 1.1). Für all diejenigen, die im

Rahmen ihrer Tätigkeit sensible Daten in speziellen Systemen des rbb verarbeiten (z. B. die Mitarbeiterinnen und Mitarbeiter der HA Personal, des Justitiariats und der Datenschutzbeauftragten) wurde die Möglichkeit für einen sicheren Zugriff auf das rbb-Netzwerk von außen eingerichtet. Zu diesem Zweck wurden an über tausend Mitarbeiter*innen Laptops ausgegeben, mit denen per sog. VPN-Tunnelung (verschlüsselte Verbindung über das Internet) eine Verbindung zu den rbb-Servern aufgebaut werden kann.

Die besondere Herausforderung beim Homeoffice besteht darin, auch bei dieser Arbeitsform die Vertraulichkeit, Integrität und Verfügbarkeit der schützenswerten Daten zu wahren. Die Gefahren, die das Arbeiten im Homeoffice in datenschutzrechtlicher Hinsicht mit sich bringt, sind nicht zu unterschätzen. Eine Gefahrenquelle stellt die Nutzung der Privatgeräte für dienstliche Zwecke dar. Für diese Geräte kann der rbb aus Kapazitätsgründen keinen Support leisten. Das bedeutet, dass der rbb auf das Sicherheitsniveau der genutzten privaten Hardware keinen unmittelbaren Einfluss hat. Zur Eindämmung dieser Risikoquelle hat der rbb spezielle Lizenzen bei Microsoft beschafft, mit denen der Zugriff auf sensitive Daten gesteuert und überwacht werden kann. Hinzu kommt beim mobilen Arbeiten generell die Gefahr, dass Unbefugte wie Familienmitglieder oder andere Mitbewohner Zugriff auf dienstliche Daten erhalten. Zur Eindämmung dieser Gefahr haben der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte umfangreiche Informationsmaßnahmen ergriffen. Zu erwähnen sind insbesondere die im Intranet veröffentlichten ausführlichen Hinweise zu den Möglichkeiten des mobilen Arbeitens unter Einhaltung von Datenschutz und Datensicherheit.

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

Im letzten Tätigkeitsbericht hatte die Datenschutzbeauftragte über den Start des ARD-Projekts „(D)ein SAP“ berichtet (15. Tätigkeitsbericht, S. 42 f.). Auf der Grundlage einer Kooperationsvereinbarung sollen alle IT-gestützten

betriebswirtschaftlichen Prozesse gemeinsam neugestaltet werden. Ziel ist es, 90% der SAP-Prozesse anstaltsübergreifend identisch zu gestalten und 70% mit Standardlösungen zu realisieren. Auch der Zentrale Beitragsservice (ZBS) ist dem SAP-Harmonisierungsprojekt beigetreten. Nach dem inzwischen gültigen „Plan B" ist der Produktivstart des Rollout-Cluster 1 (Planung, Buchung und Abrechnung von Dienstreisen) bis spätestens 01.01.2022 geplant. Um dies zu erreichen, soll die Produktivsetzung der Prozesse mit einem Piloten durchgeführt werden. Der Produktivstart dieses Piloten, der beim Mitteldeutschen Rundfunk (MDR) und Radio Bremen (RB) zum Einsatz kommen soll, ist aktuell für den 01.01.2021 vorgesehen.

Das Projekt besteht aus 29 Einzelprojekten. Nachdem das Thema Datenschutz ursprünglich zusammen mit Usability und Informationssicherheit zum Einzelprojekt 4.3 gehörte, ist es inzwischen direkt bei einem der Gesamtprojektleiter, Herrn Martin Backhaus vom MDR, angesiedelt. Die rbb-Kollegin Monika Wolf kümmert sich um die Erarbeitung der datenschutzrechtlichen Rahmenbedingungen. Sie befindet sich diesbezüglich in engem Kontakt zum AK DSB. Als ortsansässige Datenschutzbeauftragte bin ich für sie neben dem Vorsitzenden des AK DSB eine Hauptansprechpartnerin.

Im November 2019 haben die Entwicklungsarbeiten und Tests für das neue SAP-System begonnen. Das dafür genutzte System, der SAP-Solution Manager, verarbeitet derzeit noch keine Echtdaten, sondern nur fiktive Inhaltsdaten. Allerdings fallen personenbezogene Daten der mit dem System arbeitenden Projektbeteiligten an, die zur Analyse und Korrektur technischer Fehler, zur Gewährleistung der Systemsicherheit und -verfügbarkeit, zur Optimierung des Systems und zur Projektsteuerung genutzt werden. Die Datenschutzbeauftragten der beteiligten RUndfunkanstalten konnte dem Testbetrieb zustimmen, nachdem alle datenschutzrechtlich notwendigen Dokumente vorlagen. Dabei handelt es sich um folgende Dokumente:

- Ergebnis der Schutzbedarfsfeststellung des rbb-Informationssicherheitsbeauftragten,
- Systembeschreibung,

- VVT-Erfassungsbogen inklusive einer Stellungnahme zur Informationssicherheit durch den stellvertretenden Informationssicherheitsbeauftragten des IVZ sowie
- alle notwendigen Auftragsverarbeitungsverträge.

Allerdings ist anzumerken, dass SAP sich nicht auf den ARD-Mustervertrag zur Auftragsverarbeitung eingelassen hat. Für den Testbetrieb wurde das SAP-Dokument zur Auftragsverarbeitung akzeptiert. Für den Regelbetrieb muss aber alles unternommen werden, um unseren eigenen Vertrag durchzusetzen.

Am 14.11.2019 hat die rbb-Datenschutzbeauftragte beim Deutschlandradio (DLR) gemeinsam mit dem betrieblichen Datenschutzbeauftragten des MDR, Herrn Matthias Meincke, eine Datenschutz-Schulung für die Gesamtprojektmanager und alle Einzel-Projektleiter*innen durchgeführt. Ziel war die Vermittlung der datenschutzrechtlichen Grundsätze, die bei der Erarbeitung der Konzepte von vornherein mitberücksichtigt werden müssen. Einen besonderen Schwerpunkt bildeten die Themen Berechtigungs- und Löschkonzept.

Ende 2019 wurde beschlossen, dass das Informationsverarbeitungszentrum (IVZ) die Steuerung der Vereinheitlichung der SAP-Prozesse übernehmen wird. Derzeit bereitet das Projekt unter Beteiligung des AK DSB und der Informationssicherheitsbeauftragten der ARD erste EU-Ausschreibungen für (D)ein SAP vor. Dabei wird es u.a. um die Frage gehen, inwieweit Cloud-Technologien zum Einsatz kommen können.

4. Neues Ausweis- und Berechtigungsmanagementsystem

Wie berichtet (15. Tätigkeitsbericht S. 44 f.), beabsichtigt der rbb, im Rahmen des Projektes „Sicherheitskonzept“ durch die Umsetzung baulicher, technischer und organisatorischer Maßnahmen die Sicherheit in den Gebäuden und auf dem Betriebsgelände des rbb zu erhöhen. In der ersten Phase des Projekts wurden im Sommer 2019 in den Zugangsbereichen FSZ und HdR Personenvereinzelungsanlagen

errichtet. Die bisher genutzte Hausausweisdatenbank konnte die fachlichen Anforderungen, die an diese komplexe Zutritts- und Berechtigungsverwaltung gestellt werden, nicht erfüllen. Vor diesem Hintergrund hat der rbb ein professionelles Ausweis- und Berechtigungsmanagementsystem beschafft. Mit diesem System werden nun die Verwaltung der Personaldaten und Zutrittsberechtigungen, die Steuerung der Zugangsanlagen und die Erstellung der neuen elektronischen Hausausweise durchgeführt.

Alle notwendigen Dokumente für die Zutritts- und Berechtigungsverwaltung wurden in Zusammenarbeit mit der Datenschutzbeauftragten erstellt. Mit der Herstellerfirma wurden Vereinbarungen zur Auftragsverarbeitung abgeschlossen, da sie auch die Wartung des Systems übernimmt.

Zu dem ursprünglich bis zum 17. 07.2019 geplanten Probebetrieb konnte aus Sicht des Datenschutzes eine Zustimmung erteilt werden. Nachdem der Probebetrieb zweimal verlängert wurde, ging das Verfahren zu Beginn des Jahres 2020 im Wesentlichen unverändert in den Regelbetrieb.

5. Neue Regelung zum Umgang mit Dienstschlüsseln

Im Zuge der Inbetriebnahme der Zutrittskontrollanlagen ist auch die Regelung zum Umgang mit Dienstschlüsseln geändert worden. Gemäß der Dienstanweisung Meldepflicht bei Verlusten und Schäden wurden Schlüssel von Diensträumen bislang in der Regel vom Empfangsdienst verwaltet. Die dauerhafte Mitnahme von Dienstschlüsseln war nur in betrieblich begründeten Fällen möglich. Seit August 2019 haben alle Beschäftigten die Möglichkeit, ihren Einzelschlüssel für ihren fest zugeordneten bzw. eigenen Arbeitsraum für den Zeitraum ihres Beschäftigungsverhältnisses auf Antrag persönlich zu verwahren, sofern keine Sicherheitsbelange dagegensprechen. Die Inanspruchnahme dieser Möglichkeit ist freiwillig. Das Recht, den Schlüssel auch weiterhin am Empfang zu belassen, bleibt unberührt. An der Anpassung der

Dienstanweisung über die Verwahrung von Gegenständen und die Meldepflicht bei Verlusten und Schäden war die Datenschutzbeauftragte beteiligt.

6. Neues Besucheranmeldesystem

Durch die Einführung der Zutrittskontrollanlagen war es notwendig geworden, auch das Verfahren für die Anmeldung von Besuchern, Auszubildenden, Praktikanten und neuen freien sowie neuen festen Mitarbeitern neu zu gestalten. Zur Gewährung des elektronischen Zutritts ist die Ausgabe von temporären Hausausweisen erforderlich. Für die Empfangsanmeldung hat der rbb daher eine browserbasierte Software angeschafft, über welches Besucher von rbb-Mitarbeiterinnen und –Mitarbeitern angemeldet werden können. Durch diese Form der Anmeldung erhalten die Empfänge eine Übersicht der Personen, welche durch die Beschäftigten des rbb zum Betreten bzw. zum Erhalt eines Hausausweises legitimiert sind. Hierdurch können die Mitarbeiter des Sicherheitsdienstes an den Empfängen zielgerichtet Personen empfangen und werden auch in die Lage versetzt, diesen Personen fachkundig zu helfen.

Alle für die Einführung notwendigen Dokumente wie Berechtigungs- und Löschkonzept, VVT-Erfassungsbogen und Datenschutzinformation sind in Zusammenarbeit mit der Datenschutzbeauftragten entstanden, sodass sie dem Probebetrieb ab 25.11.2019 zustimmen konnte. Der Probebetrieb ist bis zum 22.05.2020 befristet.

7. Datenschutzinformation für die Videokameras

Zum Schutz des Betriebseigentums vor Diebstahl und Vandalismus sowie vor Bedrohungen jedweder Art nutzt der rbb auf seinem Gelände Videokameras. Nach einer länger andauernden Klärung der Zuständigkeiten hat sich im Frühjahr 2020 die Abteilungsleiterin Gebäudemanagement/Infrastruktur einer schon länger bestehenden Forderung seitens des Datenschutzes angenommen und einen konkreten Vorschlag für die Umsetzung der Verpflichtung nach DSGVO zur Datenschutzinformation für die Videokameras gemacht. Ein entsprechender Text an den Kameras mit Verweis

auf eine ausführliche Erläuterung im Internet ist mit der Datenschutzbeauftragten abgestimmt und wird in Kürze veröffentlicht.

8. Print at Work - Druckermanagementsystem

Ende 2018 hatte die Geschäftsleitung die Abteilung OUI damit beauftragt, den Gerätepark insgesamt zu optimieren und zukünftig auf Arbeitsplatzdrucker weitgehend zu verzichten (s. dazu 15. Tätigkeitsbericht, S. 46 ff.). Im Oktober 2019 konnte der Zuschlag für die Anmietung von Druckern und Multifunktionsgeräten inkl. „Full-Service" für mindestens fünf Jahre an einen Dienstleister erteilt werden. Der rbb wurde mit fünf verschiedenen Gerätetypen mit den Funktionen „Scannen, Drucken, Faxen und Kopieren" beliefert. Der Dienstleister ist auch für den Support, die Wartung und Reparatur der Geräte zuständig. Das mitgelieferte Druckermanagementsystem unterstützt dabei alle Prozesse von der Installation über die Konfiguration bis hin zum laufenden Betrieb. Aus Datenschutzsicht zu begrüßen ist die Tatsache, dass mit den neuen Geräten ein vertrauliches Drucken möglich ist. Das heißt, dass beliebig viele Druckaufträge online an einen Drucker abgeschickt und erst später vor Ort zum Druck freigegeben werden können. Zur Authentifizierung muss der Hausausweis an ein Lesegerät gehalten werden. Die Datei selbst bleibt bis zur Abholung auf einem sicheren Server. Wird ein Druckauftrag nicht ausgelöst, so wird er nach 24 Stunden automatisch gelöscht. Die Möglichkeit des vertraulichen Drucks ist deshalb besonders wichtig, weil Arbeitsplatzdrucker weitgehend abgeschafft wurden. Die neuen Geräte befinden sich auf zentralen Druckerinseln und werden von mehreren Personen bzw. Bereichen gemeinsam genutzt. Bei der Erarbeitung der für den Betrieb aus Datenschutzsicht notwendigen Dokumente hat die Datenschutzbeauftragte das Projektteam unterstützt. Dabei handelt es sich u. a. um die beiden VVT-Erfassungsbögen für die Nutzung der Geräte und für das Druckermanagementsystem. Der Probebetrieb ist bis zum 30.04.2020 befristet.

9. Unified Communication

In meinen letzten Tätigkeitsberichten hat die Datenschutzbeauftragte über die probeweise Einführung des Kommunikationsdienstes „Unified Communication“ (UC) berichtet (zuletzt 15. Tätigkeitsbericht, S. 43 f.). Zusätzlich zu den Funktionen einer herkömmlichen Telefonanlage, die in der Dienstvereinbarung Telekommunikationsanlagenverbund beschrieben sind, bietet UC verschiedene weitere Leistungsmerkmale, die u. a. Telefonkonferenzen und Videotelefonie sowie Chat-Funktionen umfassen. Auf der Grundlage der von der ARGE Rundfunk-Betriebstechnik (RBT) durchgeführten Schutzbedarfsfeststellung und des ebenfalls von der RBT nach BSI-Grundschutz-Standard erstellten Informationssicherheitskonzepts konnte seitens des Datenschutzes im Jahr 2018 dem Probebetrieb zugestimmt werden. Der Probebetrieb mit einer Teilnehmeranzahl von 100 Personen war zunächst bis zum 31.12.2018 befristet. Er wurde bis zum 30.06.2019 verlängert und auf weitere ca. 100 Personen erweitert. Es folgte eine abermalige Verlängerung des Probebetriebs bis zum 31.12.2019. Gleichzeitig wurde die Teilnehmerzahl am Probebetrieb um weitere 200 Personen erhöht. Erst Anfang 2020 ist mit der verabredeten Evaluation des Probebetriebs begonnen worden. Mit den Arbeiten am Entwurf einer Dienstvereinbarung ist ebenfalls erst vor kurzem begonnen worden. Bis heute konnte das Verfahren nicht in das VVT aufgenommen werden, da es immer noch an der längst angeforderten notwendigen Dokumentation fehlt. Dessen ungeachtet hat der Personalrat dem Antrag vom 10.12.2019 auf eine weitere Verlängerung des Probebetriebs bis zum 30. 06.2020 zugestimmt.

10. Neues Materialdispositionssystem

Wie in früheren Tätigkeitsberichten mitgeteilt, befindet sich seit 2017 das Materialdispositionssytem „Easyjob“ im Testbetrieb beim rbb. Die notwendigen Tests konnten aufgrund verschiedener Umstände noch nicht abgeschlossen werden. Inzwischen wurde entschieden, dass ARD-weit ein einheitliches Materialdispositionssystem

eingeführt werden soll. Zu diesem Zweck wurde ein ARD-Projekt ins Leben gerufen, bei dem der NDR die Federführung hat. Der rbb hat sich diesem Projekt angeschlossen. Die Ausschreibung konnte Ende 2019 abgeschlossen werden. Danach hat „Easyjob" den Zuschlag erhalten. Vor diesem Hintergrund wurde der Testbetrieb im rbb bis zum 31.12.2020 verlängert.

IV. Beschäftigtendatenschutz

1. SAP-Web-Anwendung xSS

Im Herbst 2019 hat der rbb für das elektronische An- und Abwesenheitsmanagement die Lotus Notes-basierte L-Net Anwendung abgelöst und durch eine SAP Web-Anwendung (xSS Abwesenheit, Teamkalender, Arbeitszeiterfassung und Beantragung Urlaub und Freizeitausgleich) ersetzt (s. auch 15. Tätigkeitsbericht, S. 49 ff.). Damit können alle Arbeitnehmer*innen ihren Urlaub und Ausgleich aus dem Freizeitkonto über eine Web-Anwendung beantragen. Zusätzlich können auch Arbeitszeit bzw. zuschlagspflichtige Arbeitstage in dem System erfasst werden. Somit wurden die bisher sehr heterogen gestalteten Prozesse in einem System (SAP) zusammengeführt, was die Übertragungsfehleranfälligkeit deutlich reduziert und die Aktualität der Daten deutlich erhöht hat.

Auf der Grundlage der vorliegenden notwendigen datenschutzrelevanten Dokumente wie Schutzbedarfsfeststellung, Stellungnahme des Informationssicherheitsbeauftragten, ausgefüllte VVT-Erfassungsbögen konnte dem Probebetrieb seitens des Datenschutzes zugestimmt werden.

Anfang 2020 erreichte die Datenschutzbeauftragte zu dem neuen System eine Beschwerde aus der Mitarbeiterschaft. Unter anderem stellte sich heraus, dass die Abwesenheitszeiten – anders als verabredet und bei dem Dienstleister in Auftrag gegeben – nicht pauschal als Abwesenheiten im Teamkalender sichtbar waren, sondern ausdifferenziert nach Urlaub, Krankheit, Elternzeit etc.. Dieser Fehler konnte

inzwischen behoben werden. In der Beschwerde wurde außerdem beanstandet, dass der Teamkalender rückwirkend ab 01.01.2019 für das ganze Team sichtbar ist. Die Datenschutzbeauftragte hat die zuständige Bereichsleiterin gebeten zu prüfen, ob eine Unterscheidung zwischen der Sichtbarkeit für diejenigen Berechtigten, die eine lange rückwirkende Einsehbarkeit benötigen (insbesondere die Disponenten) und für die übrigen Mitglieder des Teams möglich ist. Die Bereichsleiterin hat eine entsprechende Prüfung in Aussicht gestellt. Die Beschwerde führte auch zu der Erkenntnis, dass abgeschlossene Fehlmeldungen vom Fehlmelder zurzeit zu lange rückwirkend einsehbar sind, nämlich rückwirkend bis zum 02.09.2019. Die Bereichsleiterin hat zugesagt, dass der Zeitraum der rückwirkenden Einsehbarkeit zukünftig auf vier Wochen verkürzt werden soll.

2. Dispositionssystem Malu

Zur Disposition von Personal- und Sachmitteln werden im rbb leider zurzeit unterschiedliche Verfahren mit unterschiedlichen Softwareprogrammen praktiziert. Bei Kulturradio und in der Audioproduktion kommt seit 01.01.2014 die Software Malu zum Einsatz. Diese Software war von Anfang an als Interimslösung vorgesehen. Sie wurde in kurzer Zeit eigenentwickelt und an die Bedürfnisse der Bereiche angepasst. Aus der Datenschutzbeauftragten nicht bekannten Gründen wurde Malu bis heute nicht von dem ansonsten im rbb führenden Dispositionssystem MIRAAN abgelöst. Es wäre wünschenswert, wenn die HA MIT in absehbarer Zeit eine einheitliche Lösung für die Disposition im rbb erreichen könnte.

Eine Datenschutzbeschwerde aus der Belegschaft und die Notwendigkeit, die Disposition mit Malu in das VVT aufzunehmen, führten im Februar 2020 dazu, dass sich die Datenschutzbeauftragte mit dem System noch einmal näher befasst hat. Es zeigte sich, dass es für Malu bislang kein Löschkonzept gibt. Auch ist erforderlich, das Berechtigungskonzept zu optimieren und die technischen Auswertungsmöglichkeiten zu minimieren, falls das System nicht in den nächsten Monaten abgelöst wird.

So ist z. B. die Auswertung von Fehlzeiten mit Malu nicht zulässig. Derartige Auswertungen sind der HA Personal vorbehalten und werden von ihr ausschließlich in dem System xSS durchgeführt. Hat ein Vorgesetzter einen begründeten Anlass, sich die Fehlzeiten seiner Mitarbeiter*innen genauer anzuschauen, muss er sich an die HA Personal wenden. Technisch bestehen aber sehr wohl auch Auswertungsmöglichkeiten mit dem System Malu. Die Schwächen des Systems müssen bis zu seiner Ablösung mit arbeitsorganisatorischen Anweisungen (z. B. dem Verbot, bestimmte Auswertungen durchzuführen) ausgeglichen werden. Die Datenschutzbeauftragte hat die betreffenden Bereiche eindringlich auf das Verbot eigener Fehlzeiten-Auswertungen hingewiesen und auf baldige Ablösung des Systems gedrungen.

3. Meldeportal des neuen Versicherungsmaklers der ARD

Der Norddeutsche Rundfunk (NDR) hat mit Wirkung auch für die anderen ARD-Rundfunkanstalten einen Vertrag mit einem neuen Versicherungsmakler abgeschlossen. Der Vertrag hat eine Laufzeit vom 01.07.2019 bis 31.12.2021. Betreut werden die Sach- und Transportversicherungen sowie die Haftpflichtversicherungen der Rundfunkanstalten. Der Versicherungsmakler hat den Rundfunkanstalten ein Tool zur Verfügung gestellt, über das die Rundfunkanstalten ihre Schäden eigenständig an den Versicherungsmakler melden können. Der rbb ist eine der wenigen Rundfunkanstalten, die dieses Tool bislang nicht nutzen. Ausschlaggebend ist die Tatsache, dass nach dem aktuellen Berechtigungskonzept die Versicherungsabteilungen sämtlicher beteiligter Rundfunkanstalten die nicht anonymisierten Schadensmeldungen auch der Kolleg*innen der anderen beteiligten Häuser einsehen können. Dass diese Konfiguration einen klaren Verstoß gegen den Datenschutz darstellt, hatte bereits die zuständige Fachabteilung Infrastruktur von sich aus erkannt. Bei der Datenschutzbeauftragten hatten sich die Kolleginnen lediglich eine Bestätigung ihrer Haltung eingeholt. Dieser Umstand ist insofern erfreulich, als er zeigt, wie sehr das Bewusstsein für den Datenschutz unter den Kolleg*innen inzwischen ausgeprägt ist.

4. Übermittlung von Mitarbeiterdaten im Rahmen einer Berufsunfähigkeitsversicherung

Im Herbst 2019 hat der rbb die für seine Mitarbeiter*innen vorteilhafte Möglichkeit angeboten, über die Fa. BVUK eine Versicherung zur Abdeckung des Berufsunfähigkeitsrisikos abzuschließen. Dabei tritt die BVUK als Versicherungsmakler auf und übernimmt zusätzlich die nachfolgende Verwaltung der Versicherungsverhältnisse. Zur Umsetzung eines Versicherungsverhältnisses übermittelt der rbb auf der Grundlage einer Einwilligung der Arbeitnehmerin/des Arbeitnehmers die für die Versicherung relevanten Daten an die BVUK. Von dort aus werden die Daten an die Versicherung weitergeleitet. Für den Datenaustausch zwischen BVUK und rbb wurde eine entsprechende SAP-Schnittstelle geschaffen. In die Verhandlungen mit der BVUK war die Datenschutzbeauftragte einbezogen. Ursprünglich vertrat die BVUK die Meinung, dass sie auch bei der Verwaltung der Versicherungsverhältnisse keine Auftragsverarbeitung für den rbb praktiziere, sondern die Verwaltung völlig weisungsungebunden durchführen könne. In der Diskussion mit der BVUK konnte die Datenschutzbeauftragte diese davon überzeugen, dass die Durchführung der Meldungen an die Versicherung eigentlich Aufgabe des rbb ist und die Meldungen daher in seiner Verantwortung liegen. Dies hatte zur Folge, dass sich die BVUK schließlich bereiterklärt hat, mit dem rbb eine Vereinbarung zur Auftragsverarbeitung abzuschließen. In der Konsequenz musste die BVUK gegenüber dem Informationssicherheitsbeauftragten und der Datenschutzbeauftragten darlegen, wie sie mit den Versichertendaten umgeht und ihre technischen und organisatorischen Maßnahmen zu Datenschutz und Datensicherheit offenlegen. Nachdem der Informationssicherheitsbeauftragte die Maßnahmen für ausreichend befunden und auch die SAP-Schnittstelle als unbedenklich eingestuft hatte, konnte dem Vorhaben zugestimmt werden. Es wurde darauf geachtet, dass der BVUK im Vorfeld der Informationsveranstaltungen noch keine Mitarbeiterdaten vom rbb zur Verfügung gestellt wurden. Erst nach dem bekundeten Interesse eines Mitarbeiters bzw. einer Mitarbeiterin an einer Versicherung und mit dessen/deren ausdrücklicher Einwilligung hat der rbb konkrete Daten als Basis einer ersten individuellen Beratung durch die BVUK zur Verfügung gestellt.

5. Administration von Fort- und Weiterbildungsmaßnahmen durch die ems School

Ende 2019 teilte die Abteilung Personalstrategie- und entwicklung der Datenschutzbeauftragten mit, dass sie zukünftig Teile der Seminarorganisation durch die Electronic Media Scool (ems) durchführen lassen wolle. Für die Planung von Terminen und die organisatorische Abwicklung von Seminaren benötigen die Mitarbeiter*innen der ems Zugriff auf einen gemeinsamen Arbeitsbereich im rbb. Die ems verwaltet ihre PC-Clients selbst. Damit ist kein einheitliches Sicherheitsniveau gewährleistet. Aus diesem Grund hat der rbb der ems keinen direkten Zugang auf sein Netzwerk gewährt. Die Kollegen aus der HA MIT konnten jedoch eine Lösung bereitstellen, bei der zwei sog. virtuelle rbb-Clients eingerichtet wurden, zu denen die Mitarbeiter*innen der ems per Remotedesktop eine Verbindung herstellen können. Auf diese Weise können sie sich an den virtuellen Clients mit ihrem personenbezogenen Benutzer-Account anmelden und erhalten Zugriff auf das rbb-Netzwerk. Da die ems bei der Planung und organisatorischen Abwicklung von Weiterbildungsmaßnahmen Kenntnis von personenbezogenen Beschäftigtendaten erhält, hat der rbb mit der ems eine Vereinbarung zur Auftragsverarbeitung geschlossen.

6. Schritte-Challenge

In der Zeit vom 13. bis 27.01.2020 fand beim rbb eine sog. „Schritte-Challenge" statt. Sie diente dazu, die Mitarbeiter*innen zu mehr Bewegung im Alltag anzuspornen. Die Teilnahme war selbstverständlich freiwillig. Die Mitarbeiter*innen mussten sich beim Betrieblichen Gesundheitsmanagement für die Schritte-Challenge anmelden. Anschließend haben sie eine kostenlose App von Google auf ihr Smartphone geladen, die die im Aktionszeitraum zurückgelegten Schritte aufgezeichnet hat. Nach dem Zieleinlauf haben die Teilnehmer*innen ihre Gesamtschrittzahl an das Betriebliche Gesundheitsmanagement gesandt. Der Gewinn (einen Monat lang jede Woche ein großer Obstkorb) kam der gesamten Abteilung des Siegers zugute. Die Datenschutzbeauftragte war von Anfang an skeptisch. Wann immer etwas gratis im

Internet angeboten wird, ist Vorsicht geboten. Und tatsächlich: Ein technisch versierter Mitarbeiter hat herausgefunden, dass Google bei dieser App mit verschiedenen Trackern arbeitet, die die Nutzerdaten an Dritte weiterleiten. Letztlich hatte die Datenschutzbeauftragte die Durchführung der Challenge aber für vertretbar gehalten, weil die Teilnehmer*innen wissen konnten, auf was sie sich einlassen. Darüber, dass die großen US-amerikanischen Anbieter wie Google, Facebook und Co. nicht vollständig DSGVO-konform arbeiten, hat auch der rbb in der Vergangenheit immer wieder berichtet.

7. Zulässigkeit der Weitergabe des Wählerverzeichnisses an ver.di

Ende Mai 2020 endet die Amtszeit des Personalrats, was eine Neuwahl zur Folge hat. Der neue Personalrat wird per Listenwahl gewählt. Im Vorfeld der Personalratswahl hat ver.di im März wieder eine Vorwahl als Briefwahl durchgeführt. Allen rbb-Mitarbeiter*innen wurde die Möglichkeit eingeräumt, sich an der Vorwahl zu beteiligen, um auf diese Weise die Reihenfolge der Kandidat*innen auf der offenen Liste ver.di mitzubestimmen. Zur Durchführung der Vorwahl hatte ver.di die HA Personal um Herausgabe des kompletten Wählerverzeichnisses (Vorname, Nachname, Abteilung bzw. Hauspostadresse) gebeten. In der Vergangenheit war die HA Personal einem vergleichbaren Wunsch stets nachgekommen. Aus der Belegschaft erreichte die Datenschutzbeauftragte die Anfrage, ob dieses Vorgehen datenschutzkonform sei und aufgrund welcher Rechtsgrundlage die Datenübermittlung an ver.di erfolge. Der Vorwahlvorstand hatte sein Begehren auf Art. 6 Abs. 1 f) DSGVO („berechtigtes Interesse“) gestützt. Außerdem hat er zugesichert, die Daten einmalig und ausschließlich zum Zweck des Anschreibens an die wahlberechtigten Mitarbeiter*innen zu nutzen und den entsprechenden Datensatz sofort nach Ausdruck der Etiketten zu vernichten. Da unklar war, ob die genannte Norm als geeignete Rechtsgrundlage herangezogen werden könne, hat sich die Datenschutzbeauftragte an das Justitiariat gewandt. Die Kolleginnen sind nach Prüfung zu dem Ergebnis gekommen, dass Art. 6 Abs. 1 lit. f) DSGVO als geeignete Rechtsgrundlage für die Übermittlung des Wählerverzeichnisses anzusehen sei. Die von ver.di vorgetragenen Interessen seien

berechtigt, die Übermittlung des Wählerverzeichnisses für die Durchführung der Vorwahl erforderlich und es müsse auch nicht von einem Überwiegen der Interessen der Betroffenen ausgegangen werden, zumal alle im Wählerverzeichnis aufgeführten Daten bereits im Intranet veröffentlicht seien. Angesichts dieser überzeugenden Einschätzung des Justitiariats hat die Datenschutzbeauftragte ihre datenschutzrechtlichen Bedenken zurückgenommen.

8. Datenschutz bei der Beschäftigung von Leiharbeitnehmern

Beim rbb werden derzeit in verschiedenen Bereichen (u.a. beim Bühnenaufbau, in der Lichttechnik und in der HA MIT) Leiharbeitnehmer*innen eingesetzt. Sie gelten im Verhältnis zum rbb als Beschäftigte im datenschutzrechtlichen Sinne. Daraus folgt u. a., dass sie – wie auch die Arbeitnehmer*innen und freien Mitarbeiter*innen des rbb vor Aufnahme ihrer Tätigkeit beim rbb auf den Datenschutz verpflichtet werden müssen. Für die datenschutzrechtliche Verpflichtungserklärung der Leiharbeitnehmer*innen hat die Datenschutzbeauftragte einen Entwurf erarbeitet, der allen infrage kommenden Fachbereichen zur Verfügung gestellt wurde. Ferner hat sie gegenüber den Fachbereichen darauf hingewiesen, dass der rbb bei der Verarbeitung der personenbezogenen Daten der Leiharbeitnehmer*innen – insbesondere der von den Verleihfirmen zur Verfügung gestellten Profile - Verantwortlicher i. S. v. Art 4 Ziffer 7 DSGVO ist. Es gelten die datenschutzrechtlichen Grundsätze. Danach dürfen die Profildaten nur so lange aufgehoben werden, wie dies rechtlich erforderlich ist (Datensparsamkeit). Nach dem Minimalprinzip dürfen nur diejenigen Personen im rbb von den Profildaten Kenntnis erhalten, die sie für ihre Arbeit benötigen. Die Abteilung Einkauf bewahrt die Profildaten – auch von Verleihfirmen, die keinen Zuschlag erhalten haben – aus handelsrechtlichen Grundsätzen 10 Jahre auf. Für alle anderen Stellen, an die Profildaten gehen (HA Personal, HA Finanzen, Fachabteilungen und Personalrat), gelten kürzere Aufbewahrungsfristen. Dort müssen die Profildaten derjenigen, die beim rbb nicht zum Einsatz kommen, zeitnah gelöscht werden. Die Profildaten der beim rbb zum Einsatz kommenden Leiharbeitnehmer*innen müssen dort spätestens dann gelöscht werden, wenn der Einsatz beendet ist. Die

Datenschutzbeauftragte hat schließlich darauf aufmerksam gemacht, dass die Leiharbeitnehmer*innen gemäß Art. 13 DSGVO auch eine Datenschutzinformation über die beim rbb zu ihrer Person verarbeiteten Daten erhalten müssen. Den notwendigen Inhalt einer Datenschutzinformation hat sie in einer Checkliste im Intranet veröffentlicht. Aufgrund der unterschiedlichen Einsatzorte und der zu verarbeitenden personenbezogenen Daten wurde vereinbart, dass die Fachabteilungen jeweils eigene Datenschutzinformationen erarbeiten und an die Leiharbeitnehmer*innen verteilen.

9. Mitarbeiterumfragen

Mitarbeiterumfragen spielen eine immer größere Rolle im rbb. Sie erfolgen auf unterschiedliche Weise zu den unterschiedlichsten Zwecken, wie nachfolgend ausgeführt wird.

9.1 Elektronische Umfragen

Inzwischen finden die Mitarbeiterbefragungen fast ausschließlich als Online-Befragungen statt. Der Informationssicherheitsbeauftragte und ich haben vor einiger Zeit das Online-Umfragetool des Berliner Webdienstes „LamaPoll" getestet und als DSGVO-konform eingestuft. Das hat dazu geführt, dass im rbb inzwischen viele Umfragen mit diesem Tool stattfinden. Im Berichtszeitraum wurden folgende Mitarbeiterumfragen mit LamaPoll durchgeführt:

- Mitarbeiter*innen-Abfrage im Rahmen des Veränderungsprozesses der HA MIT

  Die Mitarbeiter*innen der HA MIT waren aufgefordert mitzuteilen, wo sie sich selbst künftig sehen, in welchem Team sie ihre Kompetenzen, Erfahrungen und Fähigkeiten einbringen wollen und ob sie in einem der Teams die Rolle der/des Produkt-Owner*s übernehmen wollen. Die Teilnahme an der Umfrage war freiwillig. Rechtsgrundlage für Verarbeitung der Mitarbeiterdaten war

also die "Einwilligung" (Art. 6 Abs. 1 lit. a) DSGVO) der Mitarbeiter*innen. Darauf und auf die Möglichkeit des Widerrufs der Einwilligung wurde in der mit der Datenschutzbeauftragten gemeinsam erarbeiten Datenschutzinformation ausdrücklich hingewiesen. Technisch war sichergestellt, dass zunächst die Datenschutzinformation zur Kenntnis genommen werden musste, bevor die Einwilligung auf dieser Grundlage erteilt werden konnte. Auch die anschließende Auswertung erfolgte datenschutzkonform. An ihr war nur ein kleines Team beteiligt.

- Umfrage des Justitiariats zur Zufriedenheit mit seiner Arbeit

  Das Justitiariat hat zur Ermittlung von Verbesserungspotentialen mit Unterstützung einer Beratungsfirma eine Umfrage zur Zufriedenheit mit seiner Arbeit unter den Mitgliedern des erweiterten Führungskreises durchgeführt. Die Teilnahme war freiwillig, so dass die Verarbeitung der Mitarbeiterdaten auch in diesem Fall auf Einwilligung gestützt werden konnte. Die Umfrage wurde von der Beratungsfirma online gestellt und ausgewertet. Kenntnis von personenbezogenen Ergebnissen erhielten ausschließlich die Mitarbeiter*innen des Justitiariats. Auch in diesem Fall wurden die Hinweise zum Datenschutz mit mir gemeinsam formuliert. Mit der Beratungsfirma wurde eine Vereinbarung zur Auftragsverarbeitung abgeschlossen.

- Umfrage zur Evaluation der Perspektivgespräche für freie Mitarbeiter*innen

  Im Beschluss der Geschäftsleitung von 2015 zur Einführung von Perspektivgesprächen für freie Mitarbeiter*innen war eine Evaluation der Gespräche bis September 2019 vorgesehen. Zu diesem Zweck fand im Herbst 2019 eine anonyme Umfrage unter den freien Mitarbeiter*innen und den zuständigen Führungskräften statt. Für die Umfrage unter den freien Mitarbeiter*innen wurde das Tool LamaPoll genutzt. Dabei wurden lediglich die

Abteilung/Redaktion abgefragt, in welcher das Gespräch stattgefunden hat, um quantitative Angaben für unterschiedliche Organisationseinheiten zu erhalten. Die Daten wurden ausschließlich aggregiert verarbeitet. An die Führungskräfte wurden Fragebögen per Mail verschickt. Auch hier wurden lediglich anonyme Daten abgefragt. Die Rückläufe an die HA Personal erfolgten ebenfalls per Mail.

9.2 Umfrage per Hauspost zur Qualität der ems

Eines der jährlichen Ziele des im Justitiariat angesiedelten Beteiligungsmanagements ist eine umfassende Analyse der ems. An dieser in Potsdam angesiedelten Ausbildungsstätte für angehende Journalist*innen ist der rbb beteiligt. Um eine Vorstellung von der Qualität des Volontariats zu bekommen, hat das Beteiligungsmanagement an alle Leiter*innen der rbb-Redaktionen, die Volontariats-Absolvent*innen der ems beschäftigen, per Hauspost einen Fragebogen geschickt, der ausgefüllt ebenfalls per Hauspost wieder an das Beteiligungsmanagement zurückgesandt wurde. Zur Wahrung der Anonymität wurden die Adressaten der Umfrage dazu angehalten, Angaben zu namentlich genannten Volontär*innen zu unterlassen.

10. Datenschutzvorfall beim Versand der Gehaltsabrechnungen

Am 20.12.2019 kam es beim Versand der Gehaltsabrechnungen zu einer Verletzung des Schutzes personenbezogener Mitarbeiterdaten. Dem lag folgender Sachverhalt zugrunde:

Versehentlich waren alle Gehaltsabrechnungen, die normalerweise per Hauspost an die aktiven Mitarbeiter*innen verteilt werden, an die dem rbb bekannten Privatadressen verschickt worden. Zudem waren aufgrund eines technischen Fehlers an der Kuvertiermaschine einige Gehaltsbriefe nicht verschlossen. Bereits am Sonntag, 22.12.2019, erreichten die Datenschutzbeauftragte erste Beschwerden. In Abstimmung mit der HA Personal hat sie – wie gesetzlich vorgeschrieben - am 27.12.2019

den Vorfall an die Berliner Datenschutzbeauftragte als zuständige Aufsichtsbehörde gemeldet. Inzwischen sind die Ursachen für den Datenschutzvorfall aufgeklärt und die mit der Datenschutzbeauftragten abgestimmten Maßnahmen zur Vermeidung weiterer vergleichbarer Vorfälle umgesetzt. Im Einzelnen:

Die rbb-Gehaltsabrechnungen werden im IVZ gedruckt. Die dort eingesetzte Kuvertiermaschine wurde einer technischen Prüfung unterzogen. Der „Schwamm", welcher den physischen Kontakt zur Briefverklebung herstellt, wies Verschleißerscheinungen auf, obwohl ein technischer Check durch den Hersteller ca. drei Monaten zuvor keinen Verschleiß festgestellt hatte. Der Schwamm wurde ausgetauscht. Das IVZ-Personal wurde in die Technik eingewiesen. Zukünftig überprüft das IVZ-Personal regelmäßig vor Kuvertierung den Zustand der Kuvertiermaschine.

Es wurden vier speziell gekennzeichnete abschließbare Metallbehälter für die Poststelle angeschafft, die ausschließlich für den Transport der Gehaltsabrechnungen genutzt werden. Das Verfahren zum Transport der Gehaltsabrechnungen ist in einer mit mir abgestimmten Handlungsanweisung beschrieben. Von allen Mitarbeiter*innen der Poststelle, die noch keine Vertraulichkeitserklärung unterschrieben hatten, wurde diese nachträglich eingeholt.

Nachdem die technische Möglichkeit besteht, sich seine Gehaltsabrechnungen in xSS anzeigen zu lassen und der vertrauliche Druck seit Mitte März überall im rbb umgesetzt ist (s. III 8.) liegt die Zusage der HA Personal vor, dass der elektronische Gehaltsnachweis (eine langjährige Forderung der Datenschutzbeauftragten) nun zeitnah eingeführt wird. Das wäre aus Datenschutzsicht die einfachste Lösung, um Fehler wie die beschriebenen in Zukunft zu vermeiden.

11. Mangelndes Berechtigungskonzept für das „Active Directory“

Anfang März 2020 ging der Datenschutzbeauftragten vom Leiter der Revision folgenden Hinweis zu:

Im Zuge einer Einzelfallprüfung der IT habe sich die Revision den Bereich „Assistentinnen-Netzwerk“ innerhalb der Software Confluence näher angesehen. (Confluence ist eine kommerzielle Wiki-Software, die hauptsächlich für die Dokumentation und Kommunikation von Wissen und den Wissensaustausch in Unternehmen und Organisationen verwendet wird.) Dabei habe sie festgestellt, dass die User des Bereichs (ein eingeschränkter Kreis von Assistentinnen) über den Link „Suche von Mitarbeiterkürzeln“ einen direkten Zugang zum sog. Active Directory (AD) und somit Einblick in personenbezogene Daten aller Beschäftigten erhalten konnten.

Beim AD handelt es sich um einen Verzeichnisdienst von Microsoft für Windows-Netzwerke. Das Verzeichnis ermöglicht es, die Struktur einer Organisation nachzubilden und die Verwendung von Netzwerkressourcen oder -objekten zentral zu verwalten. Das AD wird im rbb als führendes Verzeichnis hauptsächlich zur Authentifizierung verschiedener Anwendungen im rbb wie OpenMedia und Helpmatics etc. genutzt.

Die sichtbaren personenbezogen Daten bezogen sich u.a. auf den Benutzernahmen, Nachnamen, Vornamen, Befristung des Beschäftigungsverhältnisses, Dauer des Beschäftigungsverhältnisses und Art der Tätigkeit. Auf Nachfrage in der HA MIT war zu erfahren, dass die AD-Suche für sämtliche Mitarbeiter*innen über den Browser möglich war. Einzige Voraussetzung war die Kenntnis des entsprechenden Zugangspfades. Zum großen Erstaunen war dieser datenschutzwidrige Zustand innerhalb der HA MIT bekannt. Die Datenschutzbeauftragte hat daraufhin eine sofortige Beschränkung des Zugriffs auf den Kreis der berechtigten Administrator*innen gefordert. Dieser Forderung ist die HA MIT unverzüglich nachgekommen. Damit ist der Zugriff für Unbefugte nicht mehr möglich.

V. Datenschutz bei der Produktion und im Programm

1. Filebasierte Produktion

Wie berichtet (zuletzt im 15. Tätigkeitsbericht, S. 59), nutzt der rbb seit Ende 2016 das Video Produktionssystem VPMS. Im Sommer 2017 war die Einführung von VPMS im gesamten rbb abgeschlossen. Alle Redaktionen arbeiten seither bandlos. Nachträglich - erst Ende 2017 - hatte der Systembetreiber im rbb die ARGE Rundfunk-Betriebstechnik-Ingenieurbüro von ARD und ZDF (RBT) mit der Erstellung eines Sicherheitskonzepts beauftragt. Da zunächst nicht alle im Sicherheitskonzept empfohlenen Maßnahmen umgesetzt worden waren, befand sich das System für lange Zeit im Probebetrieb. Dieser Probebetrieb wurde im Laufe der Zeit schrittweise, immer wieder entsprechend der erreichten Ausbaustufe angepasst und erweitert. Nachdem die offenen Punkte des Sicherheitskonzepts im Wesentlichen umgesetzt waren, konnte mit Zustimmung des Informationssicherheitsbeauftragten und der Datenschutzbeauftragten im Oktober 2019 der Regelbetrieb aufgenommen werden. Für die Zustimmung der Datenschutzbeauftragten waren folgende Aspekte ausschlaggebend:

Personenbezogene Daten befinden sich überwiegend als Inhalte in dem System, in den einzelnen „Files". Für diese Daten gilt das Medienprivileg. Es ist daher keine spezielle Rechtsgrundlage für die Verarbeitung dieser Daten erforderlich. Die Verarbeitung der personenbezogenen Nutzungsdaten der Mitarbeiter*innen erfolgt auf der Rechtsgrundlage § 36 rbb-Staatsvertrag i. V. m. § 18 BlnDSG i. V. m. § 26 BDSG (Arbeitnehmer*innen) bzw. Art. 6 Abs. 1 b) DSGVO (freie Mitarbeiter*innen).

Gemeinsam mit dem Fachverantwortlichen hat die Datenschutzbeauftragte den VVT-Erfassungsbogen ausgefüllt. Inzwischen liegen die notwendigen Auftragsvereinbarungen mit den beiden Wartungsfirmen vor. Eine gemeinsam mit der Datenschutzbeauftragten erarbeitete Datenschutzinformation für die Mitarbeiter*innen

ist Bestandteil der Schulungsunterlagen. Diese Information ist zusätzlich im Intranet veröffentlicht.

2. Mobile Reporting

Im letzten Tätigkeitsbericht (15. Tätigkeitsbericht, S. 59 ff.) wurde darüber informiert, dass der rbb im Herbst 2018 zusätzlich zu der herkömmlichen Produktionsform das Mobile Reporting (= das Produzieren von TV-Beiträgen mit dem Smartphone) eingeführt hat. Reporter*innen drehen mit dem Smartphone und schneiden das Material anschließend mit dem Laptop selbst.

Die Datenschutzbeauftragte hatte dem Probebetrieb seinerzeit zugestimmt. Ausschlaggebend war, dass beim Mobile Reporting ausschließlich rbb-Geräte zum Einsatz kommen. Diese sind durch das sog. „Mobile Device Management" (Mobilgeräteverwaltung) geschützt. Die zentrale Verwaltung umfasst die Inventarisierung, die Software-, Daten- und Richtlinienverteilung sowie den Schutz der Daten auf den Geräten.

In den von der Datenschutzbeauftragten Ende 2018 abgehaltenen Schulungen zum Datenschutz und Recht am eigenen Bild wurde deutlich, dass einige der Kameraleute und Reporter bei der Nutzung eines iPhones auf den EB-Einheiten verunsichert sind. Sie befürchten eine Übermittlung ihrer Bewegungsdaten und des Anrufverlaufs an den Gerätehersteller Apple sowie unbemerkte Ton- und Bildaufzeichnungen über ihre eigene Person durch das Gerät. Aus diesem Grund hatte ich die zuständige OUI (jetzt HA MIT) darum gebeten, die Konfiguration der mobilen Dienstgeräte transparent zu machen. Im Herbst 2019 hatten wir damit begonnen, konkrete Hinweise zur datenschutzfreundlichen Nutzung der Geräte für die Nutzer zu formulieren. Es stellte sich heraus, dass die im Einsatz befindlichen mobilen Dienstgeräte für ganz unterschiedliche Zwecke eingesetzt werden.

Da bislang nicht klar ist, welche Anforderungen die jeweiligen Nutzergruppen haben, konnten noch keine Vorgaben für die technische Konfiguration definiert werden. Das Vorhaben hat sich aufgrund der Neustrukturierung der technischen Bereiche im Herbst/Winter 2019 verzögert. Für das Mobile Reporting ist die sichere Nutzung mittels Mobile Device Management vorgegeben. Apps können grundsätzlich nur gemeinsam nach Prüfung durch den Informationssicherheitsbeauftragten freigegeben werden. Nutzer- identifizierende Apps werden auf den MoJo (=Mobile Journalist) -Sets nicht aktiviert.

Im März 2020 haben die Fachverantwortlichen beim Personalrat die Zustimmung zum Regelbetrieb beantragt. Diesem Antrag hat der Personalrat zugestimmt. Leider wurde die Datenschutzbeauftragte vor Beantragung des Regelbetriebs nicht noch einmal gehört und hatte somit keine Möglichkeit, an die Datenschutzinformation für die Nutzer*innen der mobilen Geräte, insbesondere der für die MoJos zu erinnern. Gemeinsam mit den Fachverantwortlichen und den Kollegen aus der HA MIT haben wir nun aber verabredet, die Information zur datenschutzfreundlichen Nutzung der mobilen Dienstgeräte möglichst bald fertigzustellen.

3. zibb-Messenger

Wie berichtet (15. Tätigkeitsbericht, S. 61 f.), hat die Redaktion der Fernsehsendung zibb ihre jeweiligen Angebote und Informationen seit Herbst 2018 auch über die Messenger-Dienste WhatsApp und Telegram verbreitet (sog. zibb-Messenger). Dabei hatte zibb eine echte Kommunikation in beide Richtungen eingerichtet. Neben bloßen Abstimmungen und Meinungsumfragen hatte die Redaktion auch zur Einsendung von selbst generiertem Content (Bilder, Videos, Kommentare etc.) aufgerufen, der auch in das Fernsehprogramm einfloss. Die Datenschutzbeauftragte hatte dem Probebetrieb zugestimmt. Dabei hatte sie Wert darauf gelegt, dass dem Grundsatz der Transparenz hinreichend Rechnung getragen wird. Über die Anmeldeseite zum Messenger-Dienst hatten die Nutzer auf die mit der Datenschutzbeauftragten inhaltlich

abgestimmte Datenschutzinformation und die Nutzungsbedingen Zugriff. Für eine wirksame datenschutzrechtliche Einwilligung mussten sie bei der Registrierung die Datenschutzerklärung per Checkbox akzeptieren.

Der Pilotbetrieb des zibb-Messengers lief seit April 2019 und war ursprünglich bis Dezember 2019 angesetzt.Seit dem 07.12.2019 wird der Massenversand von Nachrichten von WhatsApp nicht mehr geduldet. Das Unternehmen gab bekannt, dass die Verbreitung solcher Nachrichten ab dem 07.12.2019 verboten sei und gerichtlich gegen Unternehmen oder Personen vorgegangen werde, die die Nutzungsbedingungen missachten. Bis dahin hatte WhatsApp den Massenversand von Nachrichten über die App zwar als nicht persönliche Kommunikation verurteilt, aber weitgehend toleriert. Daraufhin hat zibb den Betrieb des zibb-Messengers zum 08.12.2019 aufgegeben.

4. zibb-Wetterwisser

Seit Sommer 2019 werden ausgewählte Zuschauer*innen in den neu gestalteten Wetterblock bei zibb als sog. Wetterwisser eingebunden. Dafür haben sie von zibb eine Wetterwarte erhalten, die Messdaten des lokalen Wetters liefert und von den Wetterwissern online an die Redaktion gesendet werden, um sie in Form von kleinen Beiträgen in die Sendung einzubinden. Die Wetterwisser stehen laut Vertrag zibb regelmäßig von Montag bis Freitag zu den üblichen Geschäftszeiten zur Verfügung, um Wetterdaten zu übermitteln. Außerdem zeichnen die Wetterwisser regelmäßig Bilder, Videos und Wetterdaten mit dem eigenen Handy in digitaler Form auf und stellen sie der Redaktion zur Verfügung. Dies geschah ursprünglich über den zibb-Messenger und erfolgt seit Einstellung seines Betriebs (siehe 3.) über die sog. ARD/ZDF-Box. Die Datenschutzbeauftragte hat bei der Gestaltung des Vertrages mit den Wetterwissern auf datenschutzkonforme Vereinbarungen und einen sicheren Übertragungsweg hingewirkt.

5. Voting- und Interaktions-Tool „meinrbb.de“

Seit Januar 2020 setzt der rbb als erster öffentlich-rechtlicher Sender das neue Voting- und Interaktions-Tool des amerikanischen Anbieters Megaphone TV „meinrbb.de“ ein. Dieses Tool bietet die Möglichkeit, mit den Zuschauer*innen in Kontakt zu treten. Die Zuschauer*innen haben die Möglichkeit, sich durch Aufrufen einer im Fernsehprogramm eingeblendeten URL auf einem zweiten Bildschirm (second screen) an der Sendung durch diverse Möglichkeiten einer Abstimmung zu beteiligen.

Bei dem Voting werden die Daten der Zuschauer*innen verschlüsselt in der durch den Dienstleister genutzten Amazon Cloud in den USA gespeichert. Die Prüfung des Informationssicherheitsbeauftragten hat ergeben, dass die technischen und organisatorischen Maßnahmen, die der Dienstleister für die Datensicherheit ergriffen hat, ausreichen.

Das ursprüngliche Konzept von Megaphone TV war nicht europarechtskonform. Es sah die Speicherung der beim Voting anfallenden Verbindungsdaten für die gesamte Dauer des Vertrages mit dem rbb vor. Eine Möglichkeit, Teildaten zu löschen, war nicht vorgesehen. Datenschutzrechtlich bedenklich war auch die vorgesehene Verknüpfung der Nutzerdaten mit ihren Daten auf Social Media-Plattformen. Außerdem war die Verwendung des Webanalyse-Tools Google Analytics vorgesehen. Dieser kostenlose Dienst von Google ist deshalb umstritten, weil er unter anderem die Herkunft der Besucher, ihre Verweildauer auf einzelnen Seiten, und die Bereiche, in denen sie am meisten klicken, registriert. Damit ist es Google möglich, ein umfassendes Benutzerprofil von Besuchern einer Webseite zu erzeugen.

Die Datenschutzbeauftragte konnte den zuständige Programmbereichsleiter davon überzeugen, dass der Einsatz dieses Tools beim rbb nur unter der Voraussetzung von Nachbesserungen im Datenschutz möglich sei. Da Megaphone TV offenbar ein großes Interesse daran hat, sich auf dem Europäischen Markt zu etablieren, konnte auf

dem Verhandlungsweg der Verzicht auf die Einbindung von Google Analytics erreicht werden. Außerdem findet keine Verknüpfung mit den Daten auf Social Media-Plattformen statt. Schließlich hat sich der rbb vertraglich zusichern lassen, dass Megaphone TV innerhalb von maximal drei Monaten ab Kooperationsbeginn die IP-Adressen spätestens nach jeweils sieben Tagen anonymisiert. Kontaktdaten werden nur mit ausdrücklicher Einwilligung der User erhoben. Alle Zusagen wurden eingehalten. Inzwischen verzichtet Megaphone TV gänzlich auf die Speicherung von IP-Adressen.

Bei der Durchsetzung der DSGVO-Standards hat die Datenschutzbeauftragte der Datenschutz-Koordinator der Programmdirektion intensiv unterstützt. An dieser Stelle hat sich das neue Datenschutz-Management im rbb mit den Datenschutz-Koordinatoren in allen Direktionen, der Intendanz und im Justitiariat bewährt. (Siehe dazu auch II 1.)
Die konkreten Verabredungen mit Megaphone TV sind in der Vereinbarung über Auftragsverarbeitung niedergelegt. Zusätzlich hat der rbb die bei Datenverarbeitungen außerhalb Europas vorgeschriebenen Standardvertragsklauseln mit Megaphone TV abgeschlossen.

6. ScribbleLive

Scribble Live ist ein Kuratierdienst, mit dem für das Online-Angebot des rbb Informationen (vorwiegend aus sozialen Netzwerken) ausgewählt, zusammengestellt und aufbereitet werden. Den Rahmenvertrag mit Scribble Live hat der Südwestrundfunk (SWR) federführend für die ARD abgeschlossen. Vertraglich ist eine datenschutzkonforme Integration von Drittanbieterinhalten vereinbart.

Schon im Frühjahr 2019 ging beim rbb die Beschwerde eines Webseiten-Nutzers ein. Dieser machte den rbb darauf aufmerksam, dass beim Aufruf der rbb-Seiten mit ScribbleLive-Blogs Verbindungen zu Dritt-Servern hergestellt werden. Eine Rückfrage bei der Online-Koordination hat ergeben, dass dieser vertragswidrige Zustand im Herbst 2018 schon einmal aufgetreten war. Damals konnte das Problem von

Scribble-Live behoben werden. Im aktuellen Fall ist ScribbleLive trotz wiederholter Aufforderung durch den Federführer SWR und durch den rbb nicht in der Lage gewesen, den vereinbarten datenschutzkonformen Zustand herzustellen, sodass beim Aufruf der rbb-Seiten mit Scribble-Liveblog auch weiterhin automatisch Verbindungen zu Facebook, Google, Twitter Co aufgebaut und personenbezogene Daten übermittelt würden. Dem rbb blieb nichts andere übrig, als mit einer sog. Vorschaltseite sicher zu stellen, dass eine Verbindung zu der Plattform erst dann aufgebaut wird, wenn sich die User aktiv dafür entscheiden (sog. Zwei-Klick-Lösung).

7. Nachbarschaftsaktion „WIR WEIHNACHTEN“

„WIR WEIHNACHTEN“ war eine weihnachtliche Programmaktion, die der rbb gemeinsam mit dem Nachbarschaftsportal nebenan.de gestaltet hat. Ziel war es, dem Problem „Vereinsamung“ an Weihnachten eine soziale Lösung entgegenzusetzen. Die Webseite wirweihnachten.de, die gemeinsam von nebenan.de und dem rbb gestaltet wurde, hat die Anbieter von privaten Weihnachtsfesten mit Teilnahmeinteressent*innen zusammengebracht. Aus diesen Treffen wurden viele spannende Geschichten und Bekanntschaften. Der rbb hat die Aktion in fast allen Fernseh- und Hörfunk-Programmen begleitet.

Vertraglich hatten der rbb und nebenan.de vereinbart, dass für die Datenverarbeitung auf der Plattform allein nebenan.de Verantwortlicher i. S.v. Art. 4 Ziff. 7 DSGVO ist. Allerdings hatte der rbb dadurch, dass er die Nutzung dieser Plattform aktiv im Rahmen der Kooperation beworben hat, eine faktische Mitverantwortung für die Datenverarbeitung. Aus diesem Grund hat sich die Datenschutzbeauftragte gemeinsam mit der Online-Koordination im Vorfeld sehr intensiv mit der geplanten Datenverarbeitung auf der Plattform auseinandergesetzt und festgestellt, dass die ursprünglichen Pläne nicht vollständig den Standards des öffentlich-rechtlichen Rundfunks entsprachen. Auf dem Verhandlungsweg konnte der rbb viele Verbesserungen im datenschutzrechtlichen Sinn erreichen. So wurde auf der Seite wirweihnachten.de auf die ursprünglich geplante Einbindung von Social Media Plug-ins wie auch auf

bestimmte Tracking-Tools verzichtet. Außerdem hat nebenan.de für nicht notwendige funktionale Cookies ein sog. Opt-In-Verfahren installiert, so dass die Nutzer*innen jeweils frei entscheiden konnten, ob sie Cookies zur Personalisierung des Angebots, für Marketing/Werbung oder für statistische Auswertungen zulassen, oder nicht.

8. Gästelistenmanagement-Tool

Wie im letzten Tätigkeitsbericht erwähnt (15. Tätigkeitsbericht, S. 62f.), befindet sich bei der Jugendwelle Radio Fritz seit 2017 ein neues Gästelistenmanagement-Tool im Probebetrieb. Das Tool ist eine Eigenentwicklung und unterstützt Fritz bei der Organisation und Durchführung von Veranstaltungen - insbesondere beim Einladen, Informieren und Erfassen von Gästen. Schon am 28.06.2017 fand eine Schutzbedarfsfeststellung der mit dem Tool verarbeiteten Gästedaten durch den Informationssicherheitsbeauftragten statt, an dem neben den Verantwortlichen von Fritz auch der stellvertretende Datenschutzbeauftragte teilnahm. Dabei wurde verabredet, dass nur die notwendigen Daten der Gäste wie Anrede, Vor- und Zuname, Firma und Mail-Adresse verarbeitet werden. Nach jeder Veranstaltung werden die Daten innerhalb einer kurzen Frist gelöscht. Nachdem Radio Fritz im Januar 2020 endlich alle datenschutzrelevanten Dokumente vorgelegt hatte, konnte die abschließende datenschutzrechtliche Freigabe erfolgen. Das Gästelistenmanagement-Tool soll nun auch in anderen Bereichen des rbb zur Anwendung kommen.

9. Datenschutz in der Abteilung Innovationsprojekte

Die Abteilung Innovationsprojekte arbeitet zusammen mit europäischen Partnern an EU-geförderten Forschungs- und Entwicklungsprojekten. Dazu führt sie regelmäßig Nutzertests mit unterschiedlichen Proband*innen durch. Die Tests werden als sog. „Labtests“ (Tests in den Räumlichkeiten des rbb) und als Feldtests gestaltet. Bei den Feldtests wird vor allem mit Online-Fragebögen gearbeitet. Da es unter anderem um die Weiterentwicklung von barrierefreien Angeboten geht, werden in diesem

Zusammenhang mitunter sensible personenbezogene Daten wie z.B. Grad der Schwerhörigkeit u.ä. verarbeitet. Auf Einladung der Abteilung hat die Datenschutzbeauftragte am 19.06.2019 mit den Kolleg*innen ausführlich ganz grundsätzlich über Datenschutz bei der Probandenakquise und bei der Durchführung der Tests gesprochen. Im Nachgang wurden die schriftlichen Datenschutzinformationen für die Nutzer*innen überarbeitet. Außerdem hat die Datenschutzbeauftragte die Abteilung inzwischen bei zahlreichen konkreten Projekten im Datenschutz unterstützt. Vielfach ist dabei das Umfragetool LamaPoll zum Einsatz gekommen (s. dazu auch IV.9).

10. Warn-App Nina des Bundesamtes für Bevölkerungsschutz

Der rbb ist rechtlich verpflichtet, Warnmeldungen des Katastrophenschutzes zu verbreiten. Dafür ist er wie alle Rundfunkanstalten an das MoWaS (modulares Warn-System) des Bundes „angeschlossen". Der rbb erhält die Warnmeldungen über seinen Agentureingang per Satellit. Diese Meldungen gehen wie alle Agenturmeldungen in das Redaktionssystem OpenMedia und müssen dann entsprechend im Hörfunk und im Fernsehen verbreitet werden.

Alle Meldungen des Katastrophenschutzes laufen parallel auch in der NINA-App des Katastrophenschutzes ein. Da für die Warnmeldungen eine sehr hohe Verfügbarkeit gebraucht wird, hat der Informationssicherheitsbeauftragte im Zuge derCorona-Pandemie vorgeschlagen, diese App auf allen Dienstgeräten als Standard zu installieren. Das hat zwei Vorteile:

1. Sollte eine Störung in der Empfangskette bestehen, erhalten die Redakteur*innen mit dem Dienstgerät trotzdem Katastrophen-Meldungen und können entsprechende Maßnahmen einleiten.
2. Die Mitarbeiter*innen werden mit dem Dienstgerät auch unterwegs über mögliche Gefahren informiert.

Die App nutzt zur statistischen Auswertung den Webanalysedienst Google Analytics. Dabei werden die IP-Adressen aber ausschließlich anonymisiert an Google Analytics übermittelt. Standortdaten und Pushnachrichten werden erst dann erfasst, wenn die

Nutzer*innen dies aktiv in der App genehmigen. Vor diesem Hintergrund konnte die Datenschutzbeauftragte der Installation der App auf den Dienstgeräten zustimmen.

11. Audiofingerprinting

Auf ARD/ZDF-Ebene wurde beschlossen, Musikmeldungen an die Verwertungsgesellschaften GEMA und GVL weitestgehend zu automatisieren und zentral auszulagern. Zu diesem Zweck wurde das durch einen externen Dienstleister betriebene sog. Audiofingerprintingsystem (AFPS) zur technischen Musiktitelerkennung ARD/ZDF-weit eingeführt. Ziel des AFPS ist es, den Befassungsaufwand mit den Musikmeldungen in den Rundfunkanstalten erheblich zu reduzieren. Federführend für das ARD/ZDF-Gesamtprojekt ist der hr. Gegenstand des rbb-internen Projektes ist der rbb-interne Anschluss an das zentral betriebene System und die Einrichtung der entsprechenden Workflows. Der externe Dienstleister wurde beauftragt, sämtliche im Programm eingesetzte Industrietonträgermusik durch den Einsatz der Fingerprinting-Technologie automatisch zu erkennen und gemäß den Anforderungen von GEMA und GVL an diese zu melden. Somit müssen im rbb künftig lediglich diejenigen Musiken erfasst und zwecks Erkennung durch das AFPS an den Dienstleister zugeliefert werden, welche noch keinen sog. Fingerprint haben. Dies betrifft insbesondere Eigen- und Auftragsmusiken oder Live-Musiken, welche nicht am Markt erhältlich sind und welche dem Dienstleister somit erst „bekannt gemacht" werden müssen. Die Workflows zur Musikmeldung im rbb haben sich daher grundlegend geändert. Im Ergebnis bedeutet dies eine Vereinfachung bzw. einen Wegfall der Aufwände für die Einsätze von Industrietonträgern in Hörfunk und Fernsehen. Dem Antrag auf Probebetrieb vom 10.10.2019 konnte die Datenschutzbeauftragte zustimmen, nachdem folgende Dokumente für das System erarbeitet und mit ihr abgestimmt worden waren:

- die Vereinbarung zur Auftragsverarbeitung mit dem Dienstleister
- die Schutzbedarfsfeststellung des Informationssicherheitsbeauftragten und
- seine Stellungnahme zur Informationssicherheit und
- der vollständig ausgefüllte Erfassungsbogen zum VVT.

Der Probebetrieb war ursprünglich bis zum 31.12.2019 befristet. Inzwischen wurde er bis zum 30.06.2020 verlängert, da für die weitere Evaluation und Etablierung der neuen Abläufe im Zusammenhang mit dem AFPS noch mehr Zeit benötigt wird.

12. Projekt HbbTV-Teletext-Mandantensystem

Das ARD Play-Out-Center (POC) hat im Frühjahr 2019 gemeinsam mit dem ARD Text und mit allen Teletexten der ARD-Rundfunkanstalten das technische Projekt „HbbTV-Teletext-Mandantensystem" gestartet. Ziel des Projektes ist die Erweiterung der bestehenden ARD-Text HbbTV-Version, so dass die Verbreitung aller Teletexte (die bereits über den klassischen Weg im Broadcast verbreitet werden) als HbbTV-Version ermöglicht wird. Am 03.04.2019 hat ein Kick-Off-Treffen mit dem Dienstleister stattgefunden, der das System entwickelt hat. Von Anfang an wurden der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte in die Planungen einbezogen. Alle datenschutzrechtlichen Dokumente wurden gemeinsam erarbeitet. Mit den Dienstleistern wurden entsprechende Vereinbarungen zur Auftragsverarbeitung abgeschlossen. Für die Nutzer*innen der HbbTV-Teletext-Angebote und für die Mitarbeiter*innen der Rundfunkanstalten, die mit dem System arbeiten, wurden mit der Datenschutzbeauftragten abgestimmte Datenschutzinformationen entworfen. Nachdem auch der Erfassungsbogen für das VVT ausgefüllt war, konnte die Datgenschutzbeauftragte dem Probebetrieb ab Anfang 2020 zustimmen.

VI. Sonstiges

1. Neue Revisions-Software

Wie berichtet, hat die interne Revision Anfang 2019 eine datenbankgestützte Software für das Revisionsmanagement angeschafft. Die Software bietet insbesondere bei der Berechnung von Unternehmensrisiken Unterstützung. Sie wird in einer Client-Server-Umgebung im Netzwerk des rbb betrieben. Da der Softwarehersteller die

Schulungen durgeführt und auch die Wartung des Systems übernommen hat, hat der rbb mit ihm eine Vereinbarung zur Auftragsverarbeitung abgeschlossen.

Nach Durchführung einer Schutzbedarfsfeststellung und Freigabe der Software durch den Informationssicherheitsbeauftragten sowie der Durchführung einer Datenschutzfolgenabschätzung (DSFA) aufgrund der zum Teil sehr sensiblen personenbezogenen Daten, die mit dem System verarbeitet werden, hat die Datenschutzbeauftragte der Aufnahme des Probebetriebs, der bis Ende 2019 befristet war, zugestimmt. Seit Anfang 2020 befindet sich das Verfahren mit Zustimmung des Informationssicherheitsbeauftragten und der Datenschutzbeauftragten im Regelbetrieb. Gemeinsam mit dem Leiter der Revision hat die Datenschutzbeauftragte den Erfassungsbogen für das VVT überarbeitet. Ein Datenschutzhinweis wurde entworfen, der inzwischen auf jeder Prüfungsankündigung vorhanden ist.

2. Datenschutz beim Rundfunkdatenschutzbeauftragten von BR, SR, WDR, Deutschlandradio und ZDF

Seit Januar 2019 nimmt der ehemalige Direktor für Recht und Unternehmensentwicklung des rbb Herr Dr. Binder gemeinsam für BR, SR, WDR, Deutschlandradio und ZDF sowie für die von diesen verantworteten Gemeinschaftseinrichtungen das Amt des Rundfunkdatenschutzbeauftragten wahr. Herr Dr. Binder hat seinen Sitz in den Räumlichkeiten der von den Mitgliedern der ARD und dem Deutschlandradio getragenen Stiftung Deutsches Rundfunkarchiv in Potsdam. Organisatorisch, administrativ und technisch wird der Rundfunkdatenschutzbeauftragten von BR, SR, WDR, Deutschlandradio und ZDF durch den rbb betreut. In datenschutzrechtlicher Hinsicht ist der rbb insoweit Auftragsdatenverarbeiter des Rundfunkdatenschutzbeauftragten, sodass ein entsprechender Vertrag zur Auftragsverarbeitung zu vereinbaren war. Dieser Vertrag sieht die strikte Trennung der für den Rundfunkdatenschutzbeauftragten zu verarbeitenden personenbezogenen Daten von den rbb-Daten und angemessene technische und organisatorische Maßnahmen zum Schutz dieser Daten gegen unbefugten Zugriff vor. An der Gestaltung der Vereinbarung zur

Auftragsverarbeitung zwischen Herrn Dr. Binder und dem rbb haben der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte mitgewirkt.

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 DLR werden die Struktur des ZBS beschrieben und seine Aufgaben von denen der dezentralen Einheiten in den jeweiligen Landesrundfunkanstalten abgegrenzt. Die aktuelle Fassung der Verwaltungsvereinbarung wurde von den Intendantinnen und Intendanten 2019 im Sommer 2019 unterzeichnet.

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 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/den behördlichen Datenschutzbeauftragten anwendbaren

Bestimmungen der DSGVO entsprechend. Seit 05.07.2018 übt Frau Katharina Aye das Amt der behördlichen Datenschutzbeauftragten des ZBS aus. Frau Aye wird durch ihren ständigen Stellvertreter Herr Christian Kruse unterstützt. Durch die Mitgliedschaft von Frau Aye und Herrn Kruse im AK DSB (s. H I.) ist ein zeitnaher Austausch zu beitragsrelevanten Themen gewährleistet.

Um größere Themen besser vorbereiten zu können, hat der AK DSB einen Unterarbeitskreis „Beitragsdatenverarbeitung" gegründet, dessen Mitglied auch die Datenschutzbeauftragte des rbb ist. Am 19.09.2019 kamen die Mitglieder des Unterarbeitsreises zu einer Sitzung beim ZBS in Köln zusammen. Auf der Tagesordnung standen das neue Löschkonzept (s. dazu II) und die Joint Controller-Vereinbarung (s. dazu III.).

II. Neues Löschkonzept beim ZBS

Bereits in ihren beiden früheren Berichten (zuletzt im 15. Tätigkeitsbericht, S. 74) hatte die Datenschutzbeauftragte über die Aktivitäten beim ZBS zur Erarbeitung eines neuen Löschkonzepts berichtet. Diese Aktivitäten, die im Rahmen des Projekts EUDAGO PRO stattfinden, bestanden im Berichtsjahr im Wesentlichen in der Erstellung des Grobkonzepts zur Datenhaltung und Datenlöschung im Beitragsdatenverarbeitungs-System RUBIN. Das Konzept wurde in Anlehnung an die DIN Norm 66398:2016-05 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten" erstellt. Es umfasst neben den regulatorischen Vorgaben zum Löschen auch ein Inventar sämtlicher relevanter Datenarten in RUBIN. Identifiziert wurden also all diejenigen Datensätze, die personenbezogene Daten enthalten. Jede dieser Datenarten wurde einer Löschklasse zugeordnet. Aufgrund der Komplexität, der diversen Abhängigkeiten und der aus den verschiedensten Gebieten stammenden Anforderungen in Bezug auf die Aufbewahrung von Daten wurde dieses Grobkonzept – neben den Wirtschaftsprüfern und dem Autoren der DIN-Norm - auch mit der Unterarbeitsgruppe des AK DSB und anschließend auch dem

gesamten AK DSB abgestimmt. In diesem Zusammenhang ist auf Folgendes hinzuweisen:

Das Datenschutzrecht gibt vor, dass Daten zu löschen sind, wenn der Zweck entfallen ist, es sei denn, einer Löschung stehen gesetzliche Pflichten, beispielsweise zur weiteren Aufbewahrung entgegen. Bei den Fragen, welche Daten einer gesetzlichen Aufbewahrungspflicht unterliegen und wie lange diese aufzubewahren sind, handelt es sich in erster Linie nicht um datenschutzrechtliche Fragestellungen. Diese sind vielmehr von den zuständigen Fachverantwortlichen zu klären. Deren Vorgaben werden von den Datenschutzbeauftragten nicht grundsätzlich hinterfragt, sondern lediglich auf Plausibilität geprüft. Das Projekt wird voraussichtlich noch bis Mitte 2021 andauern.

III. Joint-Controller-Vereinbarung ZBS

Da die Rundfunkanstalten gemeinsam für die Datenverarbeitung durch den ZBS verantwortlich sind, muss in Ergänzung zur Verwaltungsvereinbarung gemäß Art. 26 DSGVO noch eine sog. „Joint Controller-Vereinbarung" über die konkrete Verteilung von Verantwortlichkeiten geschlossen werden. Die Rundfunkdatenschutzbeauftragten haben dafür einen Entwurf erarbeitet. Dabei galt es u. a., das Bedürfnis des ZBS, nicht jegliche datenschutzrelevante Handlung mit jeder einzelnen Rundfunkastalt individuell abstimmen zu müssen, mit dem Interesse der Rundfunkanstalten an möglichst umfassender Kontrolle des ZBS in Einklang zu bringen. Zum Zeitpunkt des Redaktionsschlusses dieses Berichts war die Befassung der den Gremien von ARD, ZDF und DLR mit dem Entwurf noch nicht abgeschlossen.

IV. Neue Verwaltungspraxis bei der Befreiung von Zweitwohnungen

Das BVerfG hat in seiner Entscheidung vom 18.07.2018 zur Verfassungsmäßigkeit der Erhebung des Rundfunkbeitrags festgelegt, dass bis zur Neuregelung durch den Gesetzgeber und ab dem Tag der Urteilsverkündung diejenigen Personen auf Antrag

von der Beitragspflicht für ihre Nebenwohnungen befreit werden können, die bereits nachweislich den Rundfunkbeitrag für ihre Hauptwohnung zahlen. Wie im letzten Tätigkeitsbericht erwähnt, hat das Urteil hinsichtlich der Umsetzung eine Vielzahl von Fragen aufgeworfen (15. Tätigkeitsbericht, S. 73 ff.). Ursprünglich hatten die Rundfunkanstalten das Urteil folgendermaßen umgesetzt:

Einen Anspruch auf Befreiung hatten nur diejenigen Zweitwohnungsinhaber, die nachwiesen, dass sie selbst einen Rundfunkbeitrag für die Hauptwohnung bezahlen.

Die Befreiung konnte rückwirkend auf den Zeitpunkt der Verkündung des Urteils erfolgen.

Zum 01.11.2019 wurde das Befreiungsverfahren für Nebenwohnungen geändert. Neu ist, dass auch diejenigen von der Beitragspflicht für Nebenwohnungen befreit werden können, deren Ehepartner oder eingetragene Lebenspartner den Rundfunkbeitrag für die gemeinsame Hauptwohnung entrichten. Der Befreiungsantrag ist nunmehr binnen drei Monaten nach Vorliegen der Befreiungsvoraussetzungen, also etwa dem Einzug in eine Nebenwohnung, beim Beitragsservice zu stellen. Wird der Antrag später gestellt, erfolgt die Befreiung nicht ab dem Monat des Einzugs, sondern erst ab dem Monat der Antragstellung. Eine rückwirkende Befreiung ist nicht länger vorgesehen.

Mit dieser geänderten Befreiungspraxis für Inhaber*innen von Nebenwohnungen hat der Beitragsservice bereits im Vorgriff dem 23. RÄndStV Rechnung getragen (s.B III 1.2). Im 23. RÄndStV, der zum 01.06.2020 in Kraft treten wird, sieht § 4 a RBStV n. F. folgende Abweichungen von der bisherigen Verwaltungspraxis vor:

Es sollen sich auch diejenigen von der Beitragspflicht für Nebenwohnungen befreien lassen können, deren Ehepartner oder eingetragener Lebenspartner den Rundfunkbeitrag für die gemeinsame Hauptwohnung entrichten.

Die Befreiung erfolgt erst auf Antragstellung bzw. nur drei Monate rückwirkend, wenn der Befreiungsschuldner innerhalb von drei Monaten nach Vorliegen der Voraussetzungen die Befreiung beantragt. Die Datenschutzbeauftragte des ZBS hat die Vorbereitungen zur Umstellung der Verwaltungspraxis – einschließlich des Entwurfs der neuen Antragsformulare – datenschutzrechtlich begleitet.

V. Auskunftsersuchen und Eingaben

1. Bearbeitung 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. Ursprünglich war diese Aufgabe bei der behördlichen Datenschutzbeauftragten und ihrem Stellvertreter angesiedelt. Mit Beginn des Jahres 2019 hat der ZBS diese Aufgabe vollständig in die Hände eines gesonderten, speziell geschulten Sachbearbeitungsteams gegeben.

Der Prozess der Beauskunftung ist zweistufig ausgestaltet. In der ersten Stufe werden im Wesentlichen die aktuellen Stammdaten zu einem Beitragskonto mitgeteilt. Zugleich wird darauf hingewiesen, dass im Einzelfall weitere Daten vorhanden sein können, die bei weiterer Nachfrage zur Verfügung gestellt werden. 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 versandt.

Im Zeitraum 01.01.-31.12.2019 hat der ZBS für den rbb insgesamt **781 einfache Eingaben** bearbeitet. Davon wurden **218 elektronisch** beantragte **Datenauskünfte** erteilt. Eine **erweiterte Datenauskunft** wurde nur in **14 Fällen** beantragt und antragsgemäß erteilt. Im Vergleich dazu hatte der ZBS für den rbb im Jahr 2018

insgesamt 651 Vorgänge bearbeitet. Für das Jahr 2019 ist folglich eine Steigerung um insgesamt **144** Vorgänge im Vergleich zu 2018 zu verbuchen.

In der nachfolgenden Übersicht wird ein zusammengefasster Überblick über die monatliche Entwicklung der datenschutzrechtlichen Eingaben bzw. der entsprechend ausgelösten Briefe beim ZBS für **alle** Landesrundfunkanstalten gegeben:

Jan.	**Feb.**	**März**	**April**	**Mai**	**Juni**	**Juli**	**Aug.**	**Sep.**	**Okt.**	**Nov.**	**Dez.**
766 (181)*	611 (148)	684 (163)	534 (164)	744 (183)	486 (171)	630 (204)	621 (206)	474 (198)	580 (242)	577 (228)	1444 (178)

(* Bei den in Klammern angegebenen Werten handelt es sich um die elektronisch beantragten einfachen Datenauskünfte, bei denen vorab jeweils automatisiert ein Brief mit Zugangsdaten versandt wurde.)

Es wird deutlich, dass die Anzahl der Anträge auf Auskunft sowie der Eingaben mit Datenschutzbezug vor allem im Dezember 2019 signifikant gestiegen ist. Eine Ursache dafür ist höchstwahrscheinlich der Umstand, dass seit Dezember 2019 vor allem über die Internetseite www.hallo-meinung.de vehement zu Störungs- und Boykottaktionen gegen den Beitragseinzug und den öffentlich-rechtlichen Rundfunk aufgerufen wird. In diesem Zusammenhang werden sogar Formulare zur Beantragung von Datenauskünften zum Ausdrucken und/oder Download zur Verfügung gestellt. Kommunikativ begleitet wird dies im Rahmen einer umfassenden Kampagne in den sozialen Medien.

2. Bearbeitung durch die Datenschutzbeauftragte des rbb

Für die Zeit vom **01.01.2019 bis 31.12.2019** ergibt sich für die rbb-Datenschutzbeauftragte in Bezug auf die Beitragsdatenverarbeitung die folgende Statistik:

Auskunftsersuchen	16
Löschbegehren	3
Sonstige Schreiben	6
Unspezifische Auskunftsersuchen:	7
Unspezifische Löschbegehren:	1
Anzahl der Vorgänge im Zeitraum 01.01. bis 31.12.2019 insgesamt:	**33**

Zum Vergleich: Im Jahr 2018 wurden insgesamt **50** Eingaben im Zusammenhang mit betragsrechtlichen Eingaben durch die rbb-Datenschutzbeauftragten bearbeitet.

Die Auskunftsersuchen und Löschbegehren wurden direkt an den ZBS zur Bearbeitung abgegeben. Auf die nicht spezifischen Auskunftsersuchen und das Löschbegehren habe ich zunächst mit einem standardisierten Zwischenbescheid reagiert und um eine Spezifikation des Begehrens gebeten. Ziel dieses zweistufigen Verfahrens ist es, eine gezielte und datensparsame Abfrage innerhalb des rbb zu ermöglichen. Auf den Zwischenbescheid haben lediglich drei Personen nochmals reagiert. Davon begehrten zwei Antragsteller eine Beauskunftung in Beitragsangelegenheiten. Diese Verfahren konnten an den ZBS abgegeben werden. Einer der Antragsteller bestand auf

der Prüfung aller Bereiche im rbb, die die Datenschutzbeauftragte daraufhin veranlasst habe (s. F).

Über die zuständige Aufsichtsbehörde, die Berliner Beauftragte für Datenschutz, erreichten die rbb-Datenschutzbeauftragte **insgesamt fünfzehn Beschwerden.** Ein Verfahren mündete in einer Verwarnung.

In mehreren Fällen ging es um die Überschreitung der gesetzlich geltenden Monatsfrist zur Beantwortung der datenschutzrechtlichen Auskunftsbegehren. (Vergleichbare Beschwerden erreichten auch die Rundfunkdatenschutzbeauftragten anderer Landesrundfunkanstalten.) Diese Beschwerden waren jeweils begründet. Grund der Fristüberschreitungen war, dass diese Schreiben nach Eingang bei der elektronischen Schlagwortsuche und Postverteilung nicht als Auskunftsersuchen erkannt worden waren, da die elektronische Schlagwortsuche lediglich auf der ersten Seite der Schreiben stattfand. In all diesen Beschwerdefällen handelte es sich um Mischsachverhalte, bei denen ein datenschutzrechtliches und ein beitragsrechtliches Begehren miteinander verbunden worden war. Wenn ein Beitragsschuldner sowohl ein beitragsrechtliches als auch ein datenschutzrechtliches Begehren verfolgte und das datenschutzrechtliche Begehren weder im Betreff noch an einer anderen Stelle auf der ersten Seite erwähnte, wurde dies durch die automatische Beleglesung und Schlagwortsuche nicht erkannt mit der Folge, dass der Vorgang in einen Postkorb zur normalen Sachbearbeitung gesteuert wurde, bei dem nicht sichergestellt war, dass die Vorgänge innerhalb eines Monats bearbeitet werden. Zur Vermeidung von weiteren Fristversäumnissen wurde die Schlagwortsuche auf alle Seiten des Schreibens ausgedehnt. Außerdem wurde der Schlagwortkatalog auf weitere Begriffe ausgeweitet.

Das Beschwerdeverfahren, in dem die Berliner Datenschutzbeauftragte erstmals eine Verwarnung gemäß Art. 58 Abs. 2 b) DSGVO gegenüber dem rbb ausgesprochen hat, betraf einen Fall, in dem die Sachbearbeitung den Widerruf einer

Einzugsermächtigung übersehen hatte, so dass es zu weiteren Abbuchungen gekommen war. In ihrer Stellungnahme gegenüber der Aufsichtsbehörde hat die Datenschutzbeauftragte dargelegt, dass die Verwarnung aus ihrer Sicht unangemessen sei, da sich derartige Fehler im Massengeschäft des Rundfunkbeitragseinzugs nicht vollständig vermeiden lassen. Eine Verwarnung wäre aus Sicht der Datenschutzbeauftragten erst im Falle von strukturellen Organisationsdefiziten gerechtfertigt. Solche Organisationsdefizite lagen in diesem Fall erkennbar nicht vor. Sowohl die Berliner Datenschutzbeauftragte als auch der rbb haben den Fall zwischenzeitlich für erledigt erklärt.

E. Datenschutz im Informationsverarbeitungszentrum

I. Allgemeines

Beim rbb ist die Gemeinschaftseinrichtung Informationsverarbeitungszentrum (IVZ) der ARD-Anstalten und des DLR angesiedelt. Dort werden u.a. alle Personal- und Archivdaten für die Rundfunkanstalten verarbeitet. Das IVZ wird auch die Steuerung der Vereinheitlichung der SAP-Prozesse für den gesamten öffentlich-rechtlichen Rundfunk übernehmen (s. C III. 3.)

Ende 2018 hat das IVZ seinen Sitz vom Standort Berlin in vom rbb angemieteten Räumlichkeiten in Potsdam verlegt. Eine groβe Zweigstelle ist auch beim WDR in Köln angesiedelt. Außerdem gibt es deutschlandweit mehrere Bürostandorte. Für die Kontrolle des Datenschutzes und der Datensicherheit sind alle Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Als Datenschutzbeauftragte der Sitzanstalt ist die Datenschutzbeauftragte des rbb federführend für das IVZ zuständig.

Einmal jährlich findet beim IVZ das „Jahrestreffen IT-Sicherheit und Datenschutz“ statt. Auf diesem Treffen informieren der Geschäftsführer und der Informationssicherheitsbeauftragte des IVZ über datenschutzrelevante Themen des

zurückliegenden Jahres. Das letzte Jahrestreffen fand am 11.12.2019 per Videoschalte statt. Schwerpunkte waren die positiven Ergebnisse des 2. ISO27001-Überwachungs-Audits im Oktober 2019, die geplante Verlegung des Rechenzentrums weg von Berlin hin nach Köln Bocklemünd und das Projekt (D)einSAP. Kontrovers diskutiert wurde die Tatsache, dass künftig wohl einige (D)ein SAP-Komponenten über Clouddienste abgebildet werden müssen.

II. Mobiles Arbeiten im IVZ

Wie im letzten Tätigkeitsbericht berichtet (15. Tätigkeitsbericht S. 83 f.), hat das IVZ am 14.01.2019 ein zweijähriges Pilotprojekt „Mobiles Arbeiten" gestartet. Das Projekt soll dazu dienen, Erfahrungen zu sammeln und zu evaluieren, ob die Form des flexiblen Arbeitens für das IVZ dauerhaft infrage kommt. Die Teilnahme an dem Projekt ist den ca. 80 Mitarbeiterinnen und Mitarbeitern, die zuvor am IVZ-Standort in Berlin gearbeitet haben, vorbehalten. Es besteht weder eine Verpflichtung noch ein Rechtsanspruch auf mobile Arbeit.

Jede Mitarbeiterin und jeder Mitarbeiter erhält für die Teilnahme einen Laptop als Endgerät. Die Geräte werden einheitlich administriert, erhalten dieselben Sicherheitsvorgaben und werden einheitlich konfiguriert. Die Nutzung von Privatgeräten für dienstliche Zwecke ist verboten. Aufgrund dieser technischen Rahmenbedingungen und der datenschutzfreundlichen Nutzungsregelungen konnte die Datenschutzbeauftragte ihre Zustimmung zu dem Pilotprojekt erteilen. Das Projekt läuft noch. Negative Datenschutzaspekte sind in den regelmäßig durchgeführten Reviews nicht bekannt geworden. Derzeit wird geplant, den Piloten voraussichtlich im April 2020 auf den Standort Köln auszuweiten. Dafür und für die generelle Beurteilung des Erfolgs ist geplant, den Pilotbetrieb um ein Jahr bis 2022 zu verlängern. Der rbb konnte von den beim IVZ gesammelten Erfahrungen unmittelbar profitieren und sich bei der Festlegung der Bedingungen für das mobile Arbeiten beim rbb (insbesondere während der Corona-Pandemie) daran anlehnen.

F. Sonstige Eingaben und Beschwerden

Neben den unter D V. 2. erwähnten Beschwerden zum Datenschutz beim Beitragseinzug hat die Datenschutzbeauftragte im Berichtszeitraum **weitere 21 Eingaben** und Beschwerden aus anderen Bereichen bearbeitet. Mehrere Beschwerden bezogen sich auf die Übermittlung falscher Daten an das Finanzamt im März 2019. Über diese Meldepanne hat die Datenschutzbeauftragte in ihrem letzten Tätigkeitsbericht ausführlich berichtet (15. Tätigkeitsbericht, S. 54 f.). Vier Beschwerden erreichten die Datenschutzbeauftragte aus der Kollegenschaft im rbb. Eine Beschwerde bezog sich auf den Aushang einer Geburtstagsliste der Mitarbeiterinnen und Mitarbeiter eines Bereichs. Da nicht alle Beteiligten mit dem Aushang einverstanden waren, wurde er auf Intervention der Datenschutzbeauftragten entfernt. Eine weitere Eingabe betraf das neue Zugangskontrollsystem. Die Vermutung, es finde mit Hilfe des Systems eine Arbeitszeiterfassung statt, konnte die Datenschutzbeauftragte ausräumen, da die Hausausweise nur beim Betreten, nicht aber beim Verlassen des rbb registriert werden. Die beiden weiteren Beschwerden bezogen sich auf die Dispositionssysteme Malu und Miraan. Während die Probleme bei Malu inzwischen geklärt werden konnten (C IV 2.), dauert die Klärung für das Dispositionssystem Miraan immer noch an. Mehrere offensichtlich begründete Eingaben zur Verletzung des Rechts am eigenen Bild bzw. zur Veröffentlichung von personenbezogenen Daten wie z. B. Kontaktdaten in den Programmangeboten im rbb hat die Datenschutzbeauftragte selbst bearbeitet und eine umgehende Löschung des Bildmaterials veranlasst. Grundsätzlich gilt aber: Die Datenverarbeitung zu journalistisch-redaktionellen Zwecken unterliegt gemäß § 9 c RStV i. V. m. §19 BlnDSG i. V. m. § 36 Abs. 2 rbb-StV dem Medienprivileg – mit der Folge, dass die Datenschutzgesetze nur sehr eingeschränkt gelten. Das Datenschutzrecht wird durch das Presserecht verdrängt. Beschwerden, die auf die Verletzung des Presserechts gestützt wird, werden im rbb zuständigkeitshalber durch das Justitiariat bearbeitet. Aus diesem Grund hat die Datenschutzbeauftragte den Fall, in dem in einem Abendschau-Beitrag versehentlich für kurze Zeit eine Patientenakte eingeblendet worden war, nach sofortiger Veranlassung der Sperrung des Beitrags

im rbb-Archiv an das Justitiariat zur weiteren Bearbeitung abgegeben. Eine Beschwerde bezog sich auf das im Online-Angebot des rbb genutzte Kuratiertool „Scribble Live“ (s. C V 6.). Die sonstigen Beschwerden hatten in der Mehrzahl einzelne Formulierungen in den Datenschutzerklärungen der unterschiedlichen Online-Angebote zum Gegenstand. In den Fällen, in denen die Beschwerden begründet waren, wurden die Datenschutzerklärungen entsprechend überarbeitet.

G. Informationsmaßnahmen

Neben den in diesem Bericht an anderen Stellen bereits erwähnten Informationsmaßnahmen im Zusammenhang mit der DSGVO und den anderen spezifischen Informationsterminen haben die Datenschutzbeauftragte und ihr Stellvertreter im Berichtszeitraum folgende Datenschutzschulungen durchgeführt:

Gemeinsam mit dem Informationssicherheitsbeauftragten hat die Datenschutzbeauftragte die für die Führungskräfte obligatorische Schulung zu Datenschutz und Informationssicherheit an folgenden Terminen durchgeführt: 15.05.,13.11.,15.11. und 20.11.2019 sowie 23.01. und 29.01.2020. Normalerweise bieten der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte zwei Führungskräfteschulungen pro Jahr an. Die zusätzlichen Termine im Berichtszeitraum fanden aufgrund der Neustrukturierungen innerhalb der Produktions- und Betriebsdirektion Ende 2019 statt, da zahlreiche neue Führungskräfte ernannt worden waren und es gerade in diesen Bereichen sehr wichtig ist, die datenschutzrechtlichen Grundsätze und die notwendigen Maßnahmen zum Schutz der Informationssicherheit zu kennen.

Der stellvertretende Datenschutzbeauftragte hat gemeinsam mit jeweils unterschiedlichen Mitarbeiterinnen und Mitarbeitern der ehemaligen Abteilung OUI (jetzt HA MIT) im Berichtszeitraum an folgenden Tagen die für SAP-Nutzer obligatorische Datenschutzschulung durchgeführt: 09.04., 18.06., 13.08., 22.10. und 10.12.19 sowie 24.02.2020.

Gemeinsam mit dem Informationssicherheitsbeauftragten hat der stellvertretende Datenschutzbeauftragte am 27.09.2019 die neuen Auszubildenden in Datenschutz und Datensicherheit geschult.

Der Schulungsbedarf im Datenschutz wächst durch die Neueinführungen von technischen Systemen und die Veränderungen bei den rechtlichen Rahmenbedingungen immer weiter. Der Datenschutzbeauftragten und ihrem Stellvertreter ist es nicht länger möglich, diesen immensen Schulungsbedarf allein abzudecken. In diesem Zusammenhang sei auch der Hinweis erlaubt, dass es nach der DSGVO eigentlich nicht Aufgabe der Datenschutzbeauftragten ist, derartige Schulungen durchzuführen. Die Verantwortung dafür liegt vielmehr beim rbb als sog. Verantwortlichen im datenschutzrechtlichen Sinne. Seit vielen Jahren ist die Datenschutzbeauftragte daher mit der HA Personal zum Thema E-Learning im Datenschutz im Gespräch. Im Sommer 2019 hat die HA Personal den Bedarf endgültig anerkannt und der ems einen entsprechenden Auftrag zur Erstellung eines eLearning-Angebots im Datenschutz erteilt. Daraufhin hat die Datenschutzbeauftragte der ems als Arbeitsgrundlage ihr eigenes umfangreiches Schulungsmaterial zur Verfügung gestellt und den designierten Autoren zu einer Führungskräfteschulung beim rbb eingeladen. Beides wurde dankend angenommen. Auf den Entwurf des Storyboards für das eLearning wartet der rbb leider bis zum Redaktionsschluss dieses Tätigkeitsberichts vergeblich.

<u>Weitere Termine:</u>

- Am 28.05.2019 hat der stellvertretende Datenschutzbeauftragte ein Referat im Rahmen des Treffens aller Schwerbehindertenvertreter*innen der ARD/ZDF beim rbb gehalten.
- Am 07.08.2019 hat die Datenschutzbeauftragte vor Mitgliedern der Vereinigung der Berliner und Brandenburgischen Pressesprecher einen Vortrag zum Datenschutz und Presserecht einschließlich dem Recht am eigenen Bild gemäß Kunsturhebergesetz gehalten.

- Am 29.10.2019 hat die Datenschutzbeauftragte in den Räumlichkeiten des rbb vor einer chinesischen Delegation einen Vortrag zum Thema „Journalismus und Rechtstaatlichkeit einschließlich Datenschutz“ gehalten.

H. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten arbeiten im AK DSB zusammen. Ein wesentliches Ziel ist es dabei, den Datenschutz bei den gemeinsamen Programmangeboten und beim Beitragseinzug nach möglichst einheitlichen Kriterien und Standards – sicherzustellen. Zudem setzt das bei Beschaffungen im öffentlich-rechtlichen Rundfunk immer häufiger durchgeführte Leadbuyer-Verfahren, bei dem eine Rundfunkanstalt federführend die Verhandlungen auch für alle anderen Rundfunkanstalten führt, voraus, dass im Datenschutz alle Rundfunkanstalten das gleiche Verständnis – beispielsweise hinsichtlich des Schutzbedarfs der mit einem System zu verarbeitenden Daten – haben.

Im Berichtszeitraum hat der AK DSB unter dem Vorsitzenden des Datenschutzbeauftragten des NDR, Herrn Dr. Heiko Neuhoff, am 11./12.04.2019 bei RB in Bremen und am 07./08.11.2019 beim BR in München getagt.

Schwerpunkte der Sitzung am 11./12.04.2019 bildeten

- Umsetzungsfragen im Zusammenhang mit dem geplanten 23. RÄndStV,
- Umsetzungsfragen im Zusammenhang mit der DSGVO,
- die geplante SAP-Harmonisierung und der
- Umstieg auf Microsoft Office 365.

Auf der Sitzung am 07./8.11.2019 ging es u.a. um

- das neue Löschkonzept beim ZBS,
- den Entwurf des Joint-Controller-Vertrages für den ZBS,
- den Umstieg auf Microsoft Office 365 und
- die aktuelle Rechtsprechung des EuGH zur Verwendung von Cookies und dem „Gefällt mir"-Button von Facebook.

Außerdem hat uns die ARD.ZDF Medienakademie, eine gemeinnützige Bildungseinrichtung für den Medienbereich mit Trainingszentren in Nürnberg und Hannover, ihr E-Learning-Angebot zum Datenschutz präsentiert. Dieses Angebot ist im Auftrag von BR und ZDF entstanden. Leider ist es für den rbb nach meiner Einschätzung nicht geeignet.

II. Rundfunkdatenschutzkonferenz

Mit dem Wirksamwerden der DSGVO wurde für die meisten Rundfunkanstalten auch die datenschutzrechtliche Aufsicht gesetzlich neu geregelt. Während zuvor nur die Pflicht zur Bestellung von eigenen Rundfunkdatenschutzbeauftragten bestand, musste nun in den meisten Rundfunkanstalten jeweils ein betrieblicher Datenschutzbeauftragter und eine datenschutzrechtliche Aufsichtsbehörde neu installiert werden. BR, SR, WDR, ZDF und DLR haben inzwischen einen gemeinsamen Rundfunkdatenschutzbeauftragten als Aufsichtsbehörde. Dieses Amt wird von dem ehemaligen Direktor für Recht und Unternehmensentwicklung des rbb, Herrn Dr. Reinhart Binder, bekleidet (s. C VI 2.). Bei SWR und NDR besteht die Besonderheit, dass die jeweiligen Landesgesetze keine Bestellung von betrieblichen Datenschutzbeauftragten vorschreiben. Diese beiden Rundfunkanstalten haben eigene Rundfunkdatenschutzbeauftragte als Aufsichtsbehörden. Bei HR, RB und rbb und neuerdings auch bei der DW besteht nach wie vor eine gespaltene Kontrollzuständigkeit. Dort treten die Rundfunkdatenschutzbeauftragten nur für den journalistisch-redaktionellen Bereich an

die Stelle der staatlichen Aufsichtsbehörden. Im Übrigen verbleibt es bei der Aufsicht der staatlichen Aufsichtsbehörden. (s. A I.).

Im Mai 2019 hat sich die Rundfunkdatenschutzkonferenz (RDSK) konstituiert. Mitglieder sind ausschließlich die für die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk zuständigen Stellen. Die Datenschutzbeauftragten des HR, RB und rbb sowie DW sind als Aufsichtsbehörden für den journalistisch-redaktionellen Teil der Datenverarbeitung der jeweiligen Rundfunkanstalten Mitglieder der RDSK.

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 nach dieser Neugründung mehr auf den operativen Bereich konzentriert, kann die RDSK etwa bei Fragen nach der datenschutzrechtlichen Zulässigkeit vorab konsultiert werden oder um eine generelle Einschätzung gebeten werden. Eine Geschäftsordnung regelt die wichtigsten Fragen zur Verständigung im Wege von Beschlüssen, Entschließungen oder Empfehlungen, für Themen, für die grundsätzlich Einvernehmen angestrebt wird. Künftig sollen alle wichtigen Themen der RDSK auch auf einer eigenen Homepage veröffentlicht werden.

Folgende Sitzungen der RDSK fanden im Berichtszeitraum statt:

- Sitzung am 11.04.2019 in Bremen; Themen u. a.: Gründung der Konferenz der Rundfunkdatenschutzbeauftragten, Definition der Aufgaben der Konferenz der Rundfunkdatenschutzbeauftragten, Entwurf einer Geschäftsordnung, Personalien: Zum „Übergangsvorsitzenden“ bis zum Abschluss einer Geschäftsordnung wurde Herr Dr. Neuhoff vom NDR und zu seinem Stellvertreter Herr Schwarze vom MDR gewählt.

- Sitzung am 26.06.2019 in Bonn; Themen u. a.: Aufsichtsrechtliche Zusammenarbeit bei Gemeinschaftsvorhaben, Zusammenarbeit mit Dritten, Aufsicht über Gemeinschaftseinrichtungen und Beteiligungsunternehmen.

- Sitzung am 18.09.2019 in Köln; Themen u.a.: Verabschiedung der Geschäftsordnung, die mit Wirkung zum 01.10.2019 in Kraft getreten ist, Interne Aufbewahrungs- und Löschfristen, Austausch über die aufsichtsrechtliche Praxis, Außenauftritt der RDSK, Webanalyse/First-Party Cookies.

- Sitzung am 06./07.11.2019 in München; Themen u.a.: Datenschutzfolgenabschätzung; Austausch über die aufsichtsrechtliche Praxis, Entschließung zum SAP-Gesamtprojekt, Eckpunkte zum Einsatz cloudbasierter Office-Anwendungen.

Folgende Positionspapiere hat die RDSK im Berichtszeitraum verabschiedet:

- Positionspapier zum IP-Autostart bei der Nutzung von HbbTV - Stand Dezember 2019 (Anlage 1)

- Datenschutzrechtliche Eckpunkte zum Einsatz cloudbasierter Office-Systeme (insbesondere MS 365) – Stand Dezember 2019 (Anlage 2)

- Datenschutzbeauftragte in Gemeinschaftseinrichtungen und gemeinschaftlichen Beteiligungsunternehmen der Rundfunkanstalten – Stand Dezember 2019 (Anlage 3)

- Empfehlungen der RDSK zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten - Stand Februar 2020 (Anlage 4).

III. Zusammenarbeit der Aufsichtsbehörden

Nach dem BDSG fällt dem Bundesdatenschutzbeauftragten 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). In § 18 Abs. 1 BDSG ist zudem festgehalten, dass die Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union die nach Art. 85 und 91 DSGVO eingerichteten spezifischen Aufsichtsbehörden beteiligen, sofern diese von der Angelegenheit betroffen sind. Seit 01.01.2019 ist der Informatiker Herr Ulrich Kelber im Amt.

Im Mai 2019 hat die Datenschutzkonferenz der staatlichen Datenschutzbeauftragten (DSK) beschlossen, sich regelmäßig zweimal jährlich mit den „spezifischen" Aufsichtsstellen auszutauschen. Dazu gehören neben den Datenschutzbeauftragten der Kirchen auch die Mitglieder der RDSK. Außerdem hat sie auch ihre Arbeitskreise für die spezifischen Aufsichtsbehörden geöffnet. Durchweg akzeptieren die Arbeitskreise der DSK aber nur eine Beteiligung von Vertretern der RDSK im Rahmen eines „Gaststatus". Aus Zeitgründen war es mir im Berichtszeitraum nicht möglich, für die RDSK an den Austauschtreffen bzw. an den Sitzungen der Arbeitskreise teilzunehmen. Die RDSK war allerdings in dem meisten Sitzungen jeweils durch eine Kollegin bzw. einen Kollegenvertreten.

IV. Teilnahme an Fortbildungen und Veranstaltungen

Am 10.10.2019 hat die Datenschutzbeauftragte auf der 13. Sitzung der AG Smart-Media in Frankfurt die Position der öffentlich-rechtlichen Rundfunkanstalten zu den Auswirkungen der DSGVO auf die Zulässigkeit des IP-Autostarts und der Reichweitenmessung bei HbbTV -Angeboten unter Verwendung von Cookies vorgetragen.

Am 17.12.2020 hat sie sich im rbb zusammen mit einigen Kollegen der RDSK und der Leitung des ARD-POC mit Vertretern der privaten Rundfunkveranstalter zum Informationsaustausch über den aktuellen Rechtsrahmen für HbbTV getroffen.

Zur Erhaltung und Erweiterung ihres Fachwissens hat die Datenschutzbeauftragte im Berichtszeitraum an folgenden Fortbildungsveranstaltungen teilgenommen:

- 22.05. bis 23.05.2019 20. Datenschutzkongress 2019 Euroforum

  Auf der Agenda standen insbesondere ein Erfahrungsaustausch in der Anwendung mit der DSGVO und ein Ausblick in die weitere datenschutzrechtliche Entwicklung

- 11.11.2019 Deutscher Bühnenverein „Datenschutzrechtlicher Workshop mit Fachdiskussion“

  Im Mittelpunkt stand die Entwicklung der Gesetzgebung und Rechtsprechung.

Der Mitarbeiter der Datenschutzbeauftragten an folgenden Fortbildungen teilgenommen:

- 22.08.2019 PowerPoint – Aufbaukurs

- 16.-17.12.2019 „Das moderne Office-Management“

Sämtliche Fortbildungsveranstaltungen fanden in Berlin statt.

Berlin, im Mai 2020

gez. Anke Naujock-Simon

Anlagen:

1. Positionspapier zum IP-Autostart bei der Nutzung von HbbTV - Stand Dezember 2019

2. Datenschutzrechtliche Eckpunkte zum Einsatz cloudbasierter Office-Systeme (insbesondere MS 365) – Stand Dezember 2019

3. Datenschutzbeauftragte in Gemeinschaftseinrichtungen und gemeinschaftlichen Beteiligungsunternehmen der Rundfunkanstalten – Stand Dezember 2019

4. Empfehlungen der RDSK zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten - Stand Februar 2020

RDSK
RUNDFUNKDATENSCHUTZKONFERENZ

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

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

Die Rundfunkdatenschutzkonferenz (RDSK) vertritt dazu folgende Rechtspositionen:

1. Die Datenverarbeitung im Zusammenhang mit der Verbreitung von Rundfunkangeboten im HbbTV–Standard ist von der Öffnungsklausel in Art. 85 Abs. 2 EU-Datenschutzgrundverordnung (DSGVO) erfasst. Sie unterliegt daher der Kontrolle der rundfunkspezifischen Datenschutzaufsicht. Auch bei den Rundfunkanstalten mit einer gespaltenen Kontrollzuständigkeit (Radio Bremen, Hessischer Rundfunk, Rundfunk Berlin-Brandenburg und Deutsche Welle) sind die Angebote von einer staatlichen Aufsicht ausgenommen und unterliegen ausschließlich der Kontrolle der Datenschutzbeauftragten der Rundfunkanstalten.

2. HbbTV gehört zum gesetzlichen Auftrag der öffentlich-rechtlichen Rundfunkanstalten. Das folgt aus der verfassungsrechtlich verbrieften Bestands- und Entwicklungsgarantie des öffentlich-rechtlichen Rundfunks.

3. Der IP-Autostart ist auch nach Wirksamwerden der DSGVO rechtlich zulässig. Rechtsgrundlage für den IP-Autostart ist Art. 6 Abs. 1 lit. e) DSGVO in Verbindung mit den gesetzlichen bzw. staatsvertraglichen Aufgabenzuweisungen an die Rundfunkanstalten. Außerdem können sich die Rundfunkanstalten auch auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO („berechtigtes Interesse“) stützen.

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

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

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

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

Stand: Dezember 2019

Einsatz cloudbasierter Office-Systeme (insbes. Microsoft Office 365): Datenschutzrechtliche Eckpunkte

Auf der Grundlage eines DSGVO-konformen Vertrages[1] darf der Verantwortliche cloudbasierte Office-Systeme wie insbesondere Microsoft Office 365 nur unter den folgenden Voraussetzungen einführen und nutzen:

Organisatorisch

- Erfassung der Prozesse und Bewertung der Schutzbedarfe

Um den adäquaten Umgang mit Daten im Unternehmen festzulegen, hat der Verantwortliche die datenschutzrechtlich relevanten Prozesse zu erfassen und ihre Schutzbedarfe jeweils zu bewerten, Art. 30 DSGVO. Da es sich bei Office 365 um eine neue Technologie mit weitreichenden Konsequenzen handelt, ist grundsätzlich eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) durchzuführen. Ein Verzicht muss sorgfältig begründet werden.

Ein Schema zur Datenklassifikation schafft hierfür nicht nur eine schlüssige Basis, sondern vereinfacht auch die anschließende Umsetzung von Schutzmaßnahmen. Ein solches Schema sollte sowohl eine Vorgabe zur grundsätzlichen Einstufung der Daten als auch zur Kennzeichnung der Dateien enthalten. In Betracht kommt dabei auch eine automatisierte Kennzeichnung mit technisch vorgegebenen Speicherorten.

- Autorisierung und Authentifikation

Die für das Access und Identity Management (Autorisierung und Authentifizierung) gewählten Verfahren müssen dem Schutzbedarf und den potentiellen Gefährdungen entsprechen. Soweit ein Hersteller (wie etwa Microsoft) Autorisierung und Authentifizierung aus einer Hand bietet, hat der Verantwortliche die damit verbundenen Vorteile und Risiken sorgfältig abzuwägen.

- Private Nutzung und dienstliche Nutzung von Privatgeräten

Der Verantwortliche muss außerdem die Regeln zur privaten Nutzung von Hard- und Software festlegen. Gestattet er die private Nutzung, muss er auch berücksichtigen, dass der Mitarbeiter als privater Nutzer sein Auskunftsrecht in Bezug auf Telemetriedaten geltend machen kann.

Sofern der Verantwortliche den Zugriff auf Daten von Geräten erlaubt, die nicht in das unternehmensweite Client-Management eingebunden sind (bspw. Privatgeräte), muss er zusätzliche Maßnahmen zur Datenintegrität und Vertraulichkeit vorsehen.

---

[1] siehe dazu die Stellungnahme des AKDSB zu wichtigen vertraglichen Voraussetzungen für den Einsatz von Office 365 aus dem Jahr 2017 – noch vor Inkrafttreten der DSGVO.
Im Vorfeld ist zu klären, ob und inwiefern Microsoft als Auftragsverarbeiter oder Joint Controller handelt.

Personell

- Verbindliche Anwendungsvorgaben

Der Verantwortliche muss verbindliche Vorgaben zur Anwendung der eingesetzten Systeme erlassen, bspw. in Form von Dienstanweisungen sowie – insbesondere für frei Beschäftigte – vertraglichen Vereinbarungen. Entsprechende Regularien können technisch-betrieblich (bspw. Endgeräte-Richtlinie) oder organisatorisch (bspw. Verhaltensregeln zum Umgang mit Daten) sein. In Bezug auf Kollaborations-Funktionen sollte der Verantwortliche außerdem festlegen, welche Informationen hierüber ausgetauscht werden dürfen und welche nicht.

- Aufklärung und Sensibilisierung

Die Anwender müssen die Schutzbedürftigkeit der Daten, mit denen sie arbeiten, ebenso kennen wie die Verhaltensvorgaben. Der Verantwortliche muss deshalb solche Regeln nicht nur vorgeben, sondern auch klar kommunizieren.

Technisch

- Deaktivierung nicht benötigter Tools und Funktionen

Der Verantwortliche sollte alle nicht benötigten Tools und Funktionen deaktivieren. Da herstellerseitig (insbesondere von Microsoft) vorgesehene Sicherheitsfunktionen mit einem erheblichen Informationstransfer verbunden sein können, muss der Verantwortliche sie auf Sinnhaftigkeit und Angemessenheit prüfen. Auch Art und Umfang der Diagnosedaten zur Programmverbesserung können stark eingeschränkt werden.

- Verschlüsselung

Jedenfalls im Falle der Verarbeitung der Daten in einem Cloud-Dienst muss der Verantwortliche die Daten je nach Schutzbedarf verschlüsseln. Da der Eigentümer und Treuhänder des Schlüssels auf die Daten zugreifen kann, bedarf es dann außerdem geeigneter Vorgaben zur Schlüsselverwaltung.

Dezember 2019

Datenschutzbeauftragte in Gemeinschaftseinrichtungen und gemeinschaftlichen Beteiligungsunternehmen der Rundfunkanstalten

I. Obligatorische Benennung von Datenschutzbeauftragten

1. Gesetzliche Ausgangslage

a) Einschlägige Vorschriften

Gemäß Art. 37 Abs. 1 DSGVO ernennt der Verantwortliche „auf jeden Fall" einen Datenschutzbeauftragten, wenn
a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird,
b) die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
c) die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder 10 besteht.

Ergänzend dazu verpflichtet § 38 Abs. 1 BDSG nF. den Verantwortlichen dazu, eine/n Datenschutzbeauftragte/n zu bestellen, soweit er in der Regel mindestens zwanzig Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt (S. 1), sowie – unabhängig davon – wenn er Verarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen, oder soweit er personenbezogene Daten geschäftsmäßig zur Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet (S. 2).

b) Verbindliche Kriterien

Daraus folgt, dass in den folgenden Fällen zwingend ein/e Datenschutzbeauftragte/r zu bestellen ist:

- Verantwortlich ist eine Behörde oder öffentliche Stelle.
- Verantwortlich ist ein Unternehmen, das mehr als 20 Personen regelmäßig mit der Verarbeitung personenbezogener Daten beschäftigt.
- Das Unternehmen verarbeitet – alternativ oder kumulativ - Daten mit Bezug zu
    - Rasse
    - Herkunft
    - Politischer Meinung
    - Religion / Weltanschauung
    - Gewerkschaftszugehörigkeit
    - Gesundheit
    - Sexualleben
- Das Unternehmen verarbeitet genetische oder biometrische Daten.

- Die Kerntätigkeit des Unternehmens besteht in der Verarbeitung – auch anonymisierter – personenbezogener Daten.
- Das Unternehmen setzt mindestens einen Geschäftsprozess ein, für den eine Datenschutzfolgenabschätzung (Art. 35 DSGVO) erforderlich ist.
- Das Unternehmen setzt personenbezogene Daten zur Markt- und Meinungsforschung ein.

2. Konsequenzen

a) Rundfunkanstalten

Die Rundfunkanstalten selbst sind nach Art. 37 Abs. 1 DSGVO grundsätzlich dazu verpflichtet, eine/n Datenschutzbeauftragte/n zu bestellen: soweit es um den Beitragseinzug geht, handeln sie als Behörde, und im Übrigen sind sie in jedem Fall als „öffentliche Stelle“ zu qualifizieren.

b) Gemeinschaftseinrichtungen

aa) Gegenstand

Die Rundfunkanstalten lassen – vor allem im Verbund der ARD – zahlreiche Aktivitäten in allen Aufgabenbereichen durch gemeinsam eingerichtete und getragene, unterschiedlich konfigurierte und organisierte Stellen abwickeln. Grundlage dafür ist in der Regel jeweils eine Verwaltungsvereinbarung der an der Stelle beteiligten Rundfunkanstalten; die einzige Ausnahme ist die Funktion des Programmdirektors Deutsches Fernsehen, die unmittelbar der ARD-Staatsvertrag konstituiert.

Unabhängig von ihrer jeweiligen konkreten Ausgestaltung handelt es sich bei jeder diesen Organisationen jedoch durchweg um nichtrechtsfähige Verwaltungseinrichtungen; lediglich für Teilaspekte wie die Arbeitgebereigenschaft kann im Einzelfall eine Teilrechtsfähigkeit in Betracht kommen. Die Aktivitäten jeder Gemeinschaftseinrichtung verantwortet eine Person, der die beteiligten Rundfunkanstalten diese Funktion – zum Beispiel als (Programm-) Geschäftsführer/in, Chefredakteur/in, Leiter/in o.ä. - befristet übertragen. Die beteiligten Rundfunkanstalten finanzieren und kontrollieren auch den Etat der Gemeinschaftseinrichtung und verantworten im Außenverhältnis, insbesondere im Rechtsverkehr, deren Handeln.

bb) Gemeinschaftseinrichtungen als „öffentliche Stelle“?

Möglicherweise können diese Gemeinschaftseinrichtungen trotz ihrer fehlenden Rechtsfähigkeit als „öffentliche Stelle“ im Sinne des Art. 37 Abs. 1 lit. a) DSGVO und damit als datenschutzrechtlich „verantwortlich“ zu qualifizieren sein. Immerhin präsentieren sich etliche von ihnen – wie etwa die Programmdirektion Deutsches Fernsehen, das ARD Hauptstadtstudio Berlin, das IVZ und andere – im Außenverhältnis wie eigenständige Organisationen, und in Teilbereichen agieren sie auch durchaus so.

Eine Verantwortung im datenschutzrechtlichen Sinne lässt sich daraus jedoch nicht ableiten. Nach Art. 4 Nr. 7 DSGVO ist „Verantwortlicher“ die natürliche oder juristische Person,

Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Allein kann jedoch nur eine Organisation über die Zwecke und Mittel der Verarbeitung entscheiden, die rechtlich selbstständig ist; entsprechendes gilt für die Entscheidung „gemeinsam mit anderen", weil dieser Terminus eine rechtliche Gleichrangigkeit impliziert. Daher ist allgemein anerkannt, dass Untergliederungen wie etwa Abteilungen oder unselbstständige Zweig- bzw. Außenstellen etc. nicht unter den Begriff der „Stelle" zu subsumieren sind und daher auch nicht als „Verantwortliche" im Sinne von Art. 4 Nr. 7 in Betracht kommen.

cc) Gesetzliche Ausnahmeregelung
Die einzige Ausnahme dieser sich aus den allgemeinen Grundsätzen ergebenden Regel gilt für den Beitragsservice. Er ist zwar ebenfalls eine nichtrechtsfähige Gemeinschaftseinrichtung, auf deren Tätigkeit für die Rundfunkanstalten jedoch gemäß § 11 Abs. 1 RBStV die Vorschriften zur Auftragsverarbeitung anzuwenden sind und für die „unbeschadet der Zuständigkeit des nach Landesrecht für die Landesrundfunkanstalt zuständigen Datenschutzbeauftragten" gemäß § 11 Abs. 2 RBStV ein behördlicher Datenschutzbeauftragter zu bestellen ist.

dd) Gemeinsame Verantwortung der Rundfunkanstalten
Datenschutzrechtlich verantwortlich für die von ihnen gegründeten und finanzierten Gemeinschaftseinrichtungen sind die jeweiligen Trägeranstalten gemeinsam. Die bei ihnen bestellten Datenschutzbeauftragten sind daher grundsätzlich auch für jede Gemeinschaftseinrichtung zuständig, die die Rundfunkanstalt (mit)verantwortet. Die Einzelheiten richten sich nach den verbindlichen Absprachen zwischen den Trägeranstalten bzw. den Datenschutzbeauftragten.

c) Beteiligungsunternehmen
Beteiligungsunternehmen der Rundfunkanstalten sind „Verantwortliche" im Sinne von Art. 4 Nr. 7 DSGVO, wenn und soweit sie als juristische Personen des Privatrechts – etwa als GmbH, gGmbH oder Stiftung - organisiert sind. Die Anzahl der Anteilseigner und die konkreten Beteiligungsverhältnisse sind insoweit ebenso irrelevant wie die Frage, ob es sich um unmittelbare oder mittelbare Beteiligungen der Rundfunkanstalten handelt.

Ob diese Beteiligungsunternehmen eine/n Datenschutzbeauftragte/n zu bestellen haben, richtet sich daher nach den unter Ziff. 1 genannten gesetzlichen Kriterien. Die oder der jeweilige Verantwortliche (Geschäftsführung, Vorstand etc.) hat selbstständig zu prüfen, ob sich daraus eine entsprechende Verpflichtung ergibt.

II. Fakultative Benennung von Datenschutzbeauftragten

1. Gesetzlicher Rahmen

Die Regelungen des Art. 37 Abs. 1 DSGVO sowie von § 38 BDSG legen nur den für die Bestellung einer oder eines Datenschutzbeauftragten maßgeblichen Mindeststandard fest.

Wie Art. 37 Abs. 4 DSGVO klarstellt, kann im Übrigen jeder Verantwortliche diese Funktion auch freiwillig einrichten. Auch in diesem Fall hat die betreffende Person die sich aus Art. 37 DSGVO ergebende Rechtsstellung.

2. Mögliche Kriterien

Für die freiwillige Ernennung einer oder eines Datenschutzbeauftragten in Gemeinschaftseinrichtungen und gemeinsamen Beteiligungsunternehmen des öffentlich-rechtlichen Rundfunks sprechen generell die folgenden Gesichtspunkte:

- Treuhandfunktion
  Der öffentlich-rechtliche Rundfunk hat eine spezifische Verantwortung gegenüber der Gesellschaft. Sowohl im administrativen als auch erst recht im journalistischen Bereich hat er gleichsam die Funktion eines Gewährsträgers für Zuverlässigkeit und Integrität, gleich ob es um das Betätigungsfeld der Rundfunkanstalten selbst oder ihrer nichtrechtsfähigen Verwaltungs- bzw. Gemeinschaftseinrichtungen geht. Dieses Grundverständnis bedingt zugleich höchste Ansprüche an die Gewährleistung des Datenschutzes. Entsprechendes gilt jedenfalls für die Mehrheits-Beteiligungsunternehmen der Rundfunkanstalten.

- Vernetzung
  Der öffentlich-rechtliche Rundfunk ist – mindestens innerhalb der ARD, aber auch darüber hinaus – ein vielfältig und hochgradig vernetzter Verbund. Jede Schwachstelle kann sich auf dieses System insgesamt auswirken: unmittelbar in Gestalt entsprechender Datensicherheitsrisiken, mittelbar in Gestalt von Imageschäden. Daher gibt es ein objektives Interesse an einem Höchstmaß an geeigneten Vorkehrungen, um die Risiken zu minimieren. Dazu zählt auch die Benennung einer bzw. eines Datenschutzbeauftragten.

- Wahrnehmung in der Öffentlichkeit
  Als beitragsfinanziertes System ist der öffentlich-rechtliche Rundfunk in besonderer Weise auf die Akzeptanz der Gesellschaft angewiesen. Verstöße gegen objektivrechtliche Vorgaben können von interessierter Seite stets zur Skandalisierung instrumentalisiert werden, um diese Akzeptanz in Frage zu stellen. Dazu eignen sich nicht zuletzt Datenschutzverstöße.

Darüber hinaus gibt es einige spezifische Gründe, die es nahelegen können, für eine Gemeinschaftseinrichtung oder ein Beteiligungsunternehmen freiwillig eine/n Datenschutzbeauftragte/n zu benennen:

- Systemrelevanz
  Die Funktionsfähigkeit bzw. datenschutzrechtliche Integrität einer Gemeinschaftseinrichtung oder eines Beteiligungsunternehmens ist für das System des öffentlich-

rechtlichen Rundfunks relevant, weil sie Leistungen für die Gesamtheit oder mehrere beteiligte Rundfunkanstalten erbringt.

- Publizistische Bedeutung
  Eine Gemeinschaftseinrichtung hat eine spezifische publizistische bzw. funktionale Rolle für die Gemeinschaft, die besonders auch mit datenschutzrechtlichen Fragestellungen verbunden ist.

- Kapazität
  Eine Gemeinschaftseinrichtung ist so groß und/oder nimmt derart spezifische Aufgaben wahr, dass sie von der oder dem Datenschutzbeauftragten der federführenden Rundfunkanstalt aus zeitlichen oder inhaltlichen Gründen nicht oder nur eingeschränkt adäquat betreut werden kann.

- Spezifische Beteiligungsstruktur
  An der Gesellschaft sind Unternehmen oder Einrichtungen beteiligt, die nicht dem öffentlich-rechtlichen Rundfunk zuzuordnen sind, sodass sich – auch in datenschutzrechtlicher Hinsicht – unterschiedliche Erwartungen oder Anforderungen ergeben können.

- Präsenz vor Ort
  Eine Gemeinschaftseinrichtung ist organisatorisch und / oder räumlich faktisch so weitgehend aus den Trägeranstalten ausgegliedert, dass dies die Präsenz einer bzw. eines Datenschutzbeauftragten vor Ort nahelegt.

- Auftragnehmer für Datenverarbeitung
  Das Unternehmen verarbeitet personenbezogene Daten im Auftrag einer oder mehrerer Rundfunkanstalten oder Dritter, die sich ihrerseits vertraglich dadurch absichern, dass sie auf der Benennung einer Ansprechperson für datenschutzrechtliche Fragen bestehen (vgl. zB. Kühling/Buchner, Kommentar zu DSGVO und BDSG, 2. Aufl. 2018, Art. 37 Rn. 26)

3. Empfehlung

Zu empfehlen ist, für jede Gemeinschaftseinrichtung bzw. jede gemeinschaftliche Beteiligungsgesellschaft, auf die mindestens eines der genannten Kriterien zutrifft, eine/n eigene/n Datenschutzbeauftragte/n zu bestellen. Davon zu unterscheiden ist die Frage, ob die Funktion dann intern oder extern, haupt- oder nebenamtlich, und gegebenenfalls auch mit welchem Zeitbudget sie wahrgenommen werden soll. Dies kann, wie sonst auch, einzelfallabhängig festgelegt werden.

Dezember 2019

EMPFEHLUNGEN DER RDSK ZUM EINSATZ VON COOKIES IN ONLINE-ANGEBOTEN DER RUNDFUNKANSTALTEN

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

I. ZULÄSSIGKEIT VON COOKIES

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

1. Allgemeiner Erlaubnistatbestand: Einwilligung der betroffenen Person

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

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

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

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

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

2. Besondere Erlaubnistatbestände

a) Unbedingt erforderliche Cookies

Eine Einwilligung ist **nicht** nötig, wenn die mit dem Einsatz des Cookies verbundene Speicherung oder der Zugang zu den entsprechenden Daten unbedingt erforderlich

ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Danach bedürfen jedenfalls sogenannte ‚funktionale Cookies' keiner Einwilligung, die etwa

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

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

Die Verarbeitung personenbezogener Daten kann jedoch auch durch einen der Erlaubnistatbestände gerechtfertigt sein, die Art. 6 Abs. 1 S. 1 lit. b) bis f) DSGVO nennt. Diese betreffen jeweils sehr spezifische Konstellationen und kommen deshalb für den Einsatz von Cookies nur in besonders gelagerten Fällen in Betracht. Nach dem Urteil des EuGH vom 1.10.2019 kann das allgemeine Interesse des Verantwortlichen an einer Erfassung und Auswertung des Nutzungsverhaltens (insbesondere in den in § 15 Abs. 3 TMG genannten Fallgruppen) nicht per se als „berechtigtes Interesse" im Sinne von Art. 6 Abs. 1 S. 1 lit. f) DSGVO qualifiziert werden. Hier bedarf es einer sorgfältigen Abwägung mit den Interessen und Grundrechten der betroffenen Personen.

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

II. EMPFEHLUNGEN FÜR DIE RUNDFUNKANSTALTEN

Rechtsgrundlage prüfen

Die Rundfunkanstalten sollten jedes von ihnen eingesetzte Cookie darauf überprüfen, ob sie es auf einen Erlaubnistatbestand stützen können. Dies kann einer der in Art. 6 Abs. 1 S. 1 lit. b) – f) DSGVO genannten Tatbestände und muss ansonsten stets eine Einwilligung der betroffenen Person sein.
Die RDSK empfiehlt den Rundfunkanstalten, den Einsatz von Cookies nicht (mehr) auf § 15 Abs. 3 TMG zu stützen.

Wirksamkeit der Einwilligungserklärung sichern

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

Datenschutzerklärung/Cookie-Hinweis anpassen

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

Spezifische Aufgabe des öffentlich-rechtlichen Rundfunks erklären

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

Februar 2020