15. Tätigkeitsbericht

der Beauftragten für den Datenschutz

des

Rundfunk Berlin-Brandenburg

Berichtszeitraum:

01. April 2018 bis 31. März 2019

Dem Rundfunkrat gemäß § 38 Abs. 7 **rbb**-Staatsvertrag

vorgelegt von

Anke Naujock

Inhaltsverzeichnis

Abkürzungsverzeichnis

AK DSB	Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio
BayVGH	Bayerischer Verfassungsgerichtshof
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BKartA	Bundeskartellamt
BlnDSG	Berliner Datenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
DSFA	Datenschutz-Folgenabschätzung
DSGVO	EU-Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
EuGH	Europäischer Gerichtshof
FSZ	Fernsehzentrum
GG	Grundgesetz
GO	Geschäftsordnung
HA	Hauptabteilung
HdR	Haus des Rundfunks
HSB	ARD-Hauptstadtstudio
IVZ	Informationsverarbeitungszentrum
JAV	Jugend- und Auszubildendenvertretung
OUI	Abteilung Organisation und IT
RändStV	Rundfunkänderungsstaatsvertrag

rbb-StV	Staatsvertrag über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg (rbb-Staatsvertrag)
RBStV	Rundfunkbeitragsstaatsvertrag
RBT	Arbeitsgemeinschaft Rundfunk-Betriebstechnik
RStV	Rundfunkstaatsvertrag
TMG	Telemediengesetz
VVT	Verzeichnis von Verarbeitungstätigkeiten
ZBS	Zentraler Beitragsservice

Vorbemerkung

Seit 1995 bin ich Datenschutzbeauftragte – zunächst beim Sender Freies Berlin und seit seiner Gründung im Mai 2003 beim rbb. Ich habe diese Funktion bislang nebenamtlich ausgeübt. Die Arbeit ist mit fortschreitender Digitalisierung immer umfangreicher und komplexer geworden. Während in den ersten Jahren ein Anteil von etwa 30 % meiner Gesamtarbeitszeit auf den Datenschutz entfiel und ich mich zu 70% meinen Aufgaben im Justitiariat widmen konnte, hat sich das Verhältnis immer mehr verschoben und war am Ende ungefähr ausgeglichen. Im zurückliegenden Jahr hat der Datenschutz die 50%-Marke überschritten. Nie war die Arbeit als rbb-Datenschutzbeauftragte für mich interessanter. Das liegt natürlich in erster Linie an der neuen rechtlichen Situation:

Am 25.05.2018 ist nach einer zweijährigen Übergangszeit die EU-Datenschutz-Grundverordnung (DSGVO) in allen Mitgliedstaaten der EU wirksam geworden. Seit diesem Tag gilt ein neues EU-weit einheitliches Datenschutzrecht – auch im rbb. Insbesondere die Anforderungen an die Dokumentation und Transparenz sind erheblich gestiegen. Um diesen neuen Herausforderungen gerecht zu werden, haben wir im Projekt zur Umsetzung der DSGVO ein neues Datenschutzmanagement für den rbb entwickelt, das von der Geschäftsleitung am 24.04.2019 verabschiedet wurde. Neben der Mitarbeit im Projekt habe ich mich intensiv um die Vermittlung der Anforderungen der DSGVO in den einzelnen Bereichen des rbb gekümmert. Wie bei allen datenschutzrechtlichen Aufsichtsbehörden hat sich auch bei der rbb-Datenschutzbeauftragten die Anzahl der zu bearbeitenden Vorgänge wie Auskunftsersuchen, Löschbegehren und Beschwerden seit Wirksamwerden der DSGVO stark erhöht.

Die Umsetzungsarbeiten im Zusammenhang mit dem Wirksamwerden der DSGVO sind noch nicht vollständig abgeschlossen. Das betrifft die Anpassung von internen Regelwerken und die Überarbeitung von Vertragsmustern, Formularen und Frage-

bögen sowie die Erarbeitung von bereichsspezifischen Löschkonzepten. Auch neue Datenschutz-Schulungskonzepte müssen erarbeitet und implementiert werden.

Dies alles sind Aufgaben des Unternehmens als datenschutzrechtlich verantwortlicher Stelle im Sinne von Art. 4 Ziffer 7 DSGVO. Natürlich unterstützt die Datenschutzbeauftragte diese Arbeiten auch weiterhin mit Rat und Tat.

Die DSGVO räumt den datenschutzrechtlichen Aufsichtsbehörden umfangreichere Befugnisse als bislang zur Abhilfe datenschutzwidriger Zustände ein. Das reicht von einer Warnung bis hin zu einem vollständigen Verbot der Datenverarbeitung. Im Berichtszeitraum musste ich keine derartigen Maßnahmen ergreifen. Soweit es in Einzelfällen zu Verletzungen der Datenschutzbestimmungen gekommen ist, wurde meinen Empfehlungen in den Fachbereichen umgehend gefolgt bzw. bin ich mit den Verantwortlichen im engen Kontakt zur Behebung des Missstands.

Meinem Mitarbeiter Herrn Christoph Schneider und meinem Stellvertreter Herrn Axel Kauffmann danke ich für die großartige Unterstützung und kollegiale Zusammenarbeit. Danken möchte ich auch der Leiterin des Projekts zur Umsetzung der DSGVO Frau Britta Böcker aus der Abteilung Organisation und IT (OUI) und allen anderen Mitgliedern des Projekts für Ihr großes Engagement für den Datenschutz. Dem Personalrat danke ich auch in diesem Jahr wieder für die konstruktive und vertrauensvolle Zusammenarbeit. Bei der Bewältigung von schwierigen Situationen und Entscheidungen konnte ich mir der Rückendeckung seitens der Intendanz, der Justitiarin und der übrigen Mitglieder der Geschäftsleitung immer gewiss sein. Auch dafür möchte ich mich herzlich bedanken.

Dieser Tätigkeitsbericht wird – wie die Vorgängerberichte - nach Erstattung gegenüber dem Rundfunkrat - im Online-Angebot des rbb veröffentlicht werden.

Er wird unter

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

abrufbar sein.

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

I. Gesetzliche Grundlagen

Die Rechtsgrundlagen haben sich für die Datenschutzbeauftragte des rbb nach Wirksamwerden der DSGVO nur geringfügig geändert.

Der rbb-Staatsvertrag ist unverändert geblieben. Dass die Landesgesetzgeber von Berlin und Brandenburg keine Notwendigkeit zur Neuregelung der datenschutzrechtliche Aufsicht über den rbb gesehen haben, hat seine Ursache wohl in der Sondersituation, die es beim rbb, wie auch bei Radio Bremen (RB) und beim Hessischen Rundfunk (HR) schon vor Inkrafttreten der DSGVO gab. Nur für den journalistisch-redaktionellen Bereich trat und tritt hier die Rundfunkdatenschutzbeauftragte an die Stelle der Landesdatenschutzbeauftragten. Demgegenüber liegt die Zuständigkeit für die Datenschutzkontrolle im wirtschaftlich-administrativen Bereich bei der Landesdatenschutzbeauftragten. Diese sog. „gespaltene Kontrolle“ ist verfassungsrechtlich bedenklich, worauf die betroffenen Rundfunkanstalten in der Vergangenheit immer wieder vergeblich hingewiesen haben. Denn vielfach sind die Verwaltungstätigkeiten untrennbar mit der journalistischen Arbeit verbunden. Leider haben die zuständigen Landesgesetzgeber die durch die DSGVO eingetretene Zäsur nicht dazu genutzt, diesen Konstruktionsfehler zu korrigieren.
Nach wie vor gilt: 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-Staatsvertrags und anderer Vorschriften über den Datenschutz, soweit der rbb personenbezogene Daten zu eigenen, journalistisch-redaktionellen oder literari-

schen 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-Staatsvertrag i. V. m. § 4 Abs. 1 des an die DSGVO angepassten 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 Mitarbeiter und der diesbezüglichen Überprüfungen,
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung 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, 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 03.09.2015 hat mich der Rundfunkrat gemäß § 38 Abs. 1 rbb-StV auf Vorschlag der ehemaligen Intendantin Frau Dagmar Reim für eine weitere Amtszeit von vier Jahren rückwirkend vom 01.07.2015 bis zum 30.06.2019 zur Beauftragten für den Datenschutz beim rbb bestellt. Parallel dazu hat die Intendantin für den gleichen Zeitraum meine Bestellung zur betrieblichen Datenschutzbeauftragten gemäß § 19 a BlnDSG (*jetzt § 4 Abs. 1 BlnDSG*) entsprechend verlängert. Die Wahrnehmung der Aufgaben als Beauftragte für den Datenschutz gemäß § 38 Abs. 1 rbb-StV und als betriebliche Datenschutzbeauftragte gemäß § 4 Abs. 1 BlnDSG in einer Person ist schon deshalb notwendig, weil sich die Bereiche der journalistisch-redaktionellen und der wirtschaftlich-administrativen Tätigkeit oftmals nicht klar voneinander abgrenzen lassen.

Meine Funktion als Datenschutzbeauftragte des rbb habe ich auch im Berichtzeitraum nebenamtlich zu meiner Tätigkeit im Justitiariat wahrgenommen.

Seit 01.04.2014 ist der Mitarbeiter der Revision, Axel Kauffmann, stellvertretender behördlicher Datenschutzbeauftragter. Bei größeren Projekten beziehe ich Herrn Kauffmann von Anfang an mit ein, damit er jederzeit in der Lage ist, im Bedarfsfall für mich einzuspringen. Aufgrund des extrem hohen Arbeitsanfalls im Berichtszeitraum musste ich Herrn Kauffmann viel öfter als zurückliegend bitten, mich in Terminen zu vertreten. Daneben hat er auch wieder eine Reihe von Datenschutzschulungen übernommen und durchgeführt (s. G.)
Bis einschließlich Juli 2018 hatte eine Mitarbeiterin des Justitiariats die Sekretariatsarbeit im Datenschutz neben ihren Aufgaben im Justitiariat erledigt. Schon vor Wirksamwerden der DSGVO hatte sich gezeigt, dass sich diese Konstellation angesichts des enorm angestiegen Arbeitsanfalls bei der Datenschutzbeauftragten beim besten Willen nicht länger aufrechthalten ließ. Dazu ist für die Datenschutzbeauftragte in Umsetzung der DSGVO eine Reihe von zusätzlichen arbeitsaufwändigen

Daueraufgaben hinzugekommen (u. a. das Führen des sog. Verzeichnisses von Verarbeitungstätigkeiten).
Vor diesem Hintergrund hat die Geschäftsleitung meinen Bedarf an Unterstützung durch einen eigenen Mitarbeiter anerkannt. Seit August 2018 werde ich von Herrn Christoph Schneider unterstützt. Herr Schneider erledigt die Sekretariatsarbeit und entlastet mich auch bei der Routine-Sachbearbeitung.

B. Entwicklung des Datenschutzrechts

I. Europa

1. Normen und Abkommen

1.1 EU-Datenschutzgrundverordnung

Seit 25.05.2018 ist die DSGVO in allen EU-Mitgliedsstaaten direkt geltendes Recht. All das, was die DSGVO regelt, ist als abschließend anzusehen. Vom nationalen Gesetzgeber werden hauptsächlich nur noch Verfahrensfragen und Zuständigkeiten geregelt. Es gibt allerdings zwei Öffnungsklauseln, die dem nationalen Gesetzgeber Raum für eigene Regelungen lassen: Zum einen handelt es sich um die Öffnungsklausel zur Regelung des Medienprivilegs (Art. 85 DSGVO). Dabei geht es um den Auftrag für die Mitgliedstaaten, für den journalistischen Bereich angemessene Ausnahmeregelungen zum ansonsten strengen Datenschutzreglement zu formulieren. Die zweite Öffnungsklausel betrifft die Regelung der Beschäftigtendatenverarbeitung (Art. 88 DSGVO).

Für den rbb wird der Datenschutz bei der journalistischen Datenverarbeitung im Rundfunkstaatsvertrag (RStV), im rbb-Staatsvertrag (rbb-StV) und im neuen Berliner Datenschutzgesetz (BlnDSG) geregelt (s. III). Im Beschäftigtendatenschutz kommt über das Berliner Datenschutzgesetz § 26 des Bundesdatenschutzgesetzes (BDSG) zur Anwendung.

Zu den Änderungen durch die DSGVO s. auch 14. Tätigkeitsbericht (S. 5 ff).

1.2 ePrivacy-Verordnung

Wie im 14. Tätigkeitsbericht ausgeführt (S. 7 f.), hatte die EU-Kommission bereits im Januar 2017 einen Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation, die sog. ePrivacy-Verordnung, vorgelegt. Die Verordnung soll 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. Das Europäische Parlament hatte daraufhin im Oktober 2017 eine Verhandlungsposition zu dem Entwurf festgelegt und die Aufnahme interinstitutioneller Verhandlungen beschlossen. Allerdings fehlt bis heute die Positionierung des Europäischen Rates, um den sog. Trilog zu starten, d. h. um den Verordnungsentwurf auf europäischer Ebene zwischen Kommission, Parlament und Rat abschließend zu verhandeln und zu verabschieden. Insbesondere Österreich sperrt sich gegen ein Einwilligungserfordernis bezüglich der Nutzung von Cookies. Es wird davon ausgegangen, dass frühestens nach der Europawahl Mitte 2019 eine endgültige Fassung der ePrivacy-Verordnung vorliegen wird und diese erst im Jahr 2022 Anwendung findet.

Für den rbb wird die zukünftige ePrivacy-Verordnung vor allem für das Webtracking relevant sein. Wie die meisten anderen Website-Betreiber führt der rbb Webtracking zur Webanalyse und Reichweitenmessung durch. Nach dem bislang geltenden Telemediengesetz (TMG) waren pseudonyme Nutzungsprofile erlaubt, die nur anonyme oder pseudonyme Daten enthalten, d. h. Daten, aus denen der Anbieter nicht die Identität des Nutzers ableiten kann. Personenbezogene Nutzungsprofile waren demgegenüber nur mit ausdrücklicher Einwilligung zulässig.

In einer Positionsbestimmung vom 26.04.2018 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) festgestellt, dass die Vorschriften des TMG von der DSGVO verdrängt werden. Insofern richte-

ten sich die Anforderungen für Telemedienanbieter bis auf weiteres nach der DSGVO. Diese Position hat in der Öffentlichkeit für große Irritation gesorgt, weil der Eindruck erweckt worden war, dass Webtracking seit Wirksamwerden der DSGVO generell nur noch mit Einwilligung der Nutzer möglich sei.

Im Nachgang hat die DSK diese Position klarstellend konkretisiert. So vertritt die Berliner Datenschutzbeauftragte in ihren Veröffentlichungen die Auffassung, dass Datenverarbeitungen, die für die Bereit- und Darstellung der Webseite und zur Sicherung der Integrität der Webseite erforderlich sind, sowie bestimmte Verfahren der Webanalyse bzw. Reichweitenmessung im Rahmen einer Interessenabwägung nach Art. 6 Abs. 1 f DSGVO regelmäßig zulässig sind (Jahresbericht 2018, S. 150).

Diese Auffassung stimmt im Ergebnis mit der Position der Rundfunkdatenschutzbeauftragten überein, die von Anfang an die Meinung vertreten haben, dass jedenfalls bis zum Inkrafttreten der ePrivacy-Vorordnung der Einsatz von Cookies im bisherigen Umfang auch weiterhin erlaubt ist. Im Ergebnis besteht für die Praxis derzeit kein Änderungsbedarf.

1.3 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.

Ende 2018 hat die EU-Kommission ihren zweiten Prüfbericht zum Privacy Shield veröffentlicht. Trotz bekannter Umsetzungsdefizite ist sie erneut zu dem Ergebnis gekommen, dass unter dem Regime des Privacy Shield ein angemessenes Datenschutzniveau herrsche.

Als die Kommission mit der US-Regierung im Oktober 2018 in Brüssel zusammen kam, um die zweite Überprüfung des Privacy Shields durchzuführen, lagen konfliktreiche Monate hinter beiden Seiten. Vor allem in der Union hatte sich die Kritik an dem Abkommen signifikant erhöht, was in einem Beschluss des EU-Parlaments, es entscheidend nachzubessern oder auszusetzen und einem Beschwerdebrief der EU-Justizkommissarin an den US-Handelsminister gipfelte. Denn es hatte sich gezeigt, dass der Privacy Shield an denselben Schwächen wie das Safe Harbor Abkommen leidet.

Nach wie vor fehlen belastbare Nachweise darüber, inwieweit die Unternehmen tatsächlich die Datenschutzgrundsätze des Privacy Shields einhalten. Bürgern der EU, die über keinen Wohnsitz in den USA verfügen, steht kein Individualrechtsschutz gegen die Ausspähung ihrer Daten zu. Zwar hatte die Obama-Administration noch eine Direktive verabschiedet, welche der weltweiten Massenüberwachung Grenzen setzt und eine Gleichbehandlung von US-Staatsbürgern und Ausländern proklamiert. Diese begründet aber keine subjektiven Rechte und verfügt nicht über Gesetzeskraft. Außerdem sind Massenüberwachungsmaßnahmen weiterhin zu unbegrenzten Zwecken möglich, solange die Daten nur zeitlich begrenzt gespeichert werden. Dieser Umstand ist vor allem wegen der weiten Zugriffsbefugnisse der US-Nachrichtendienste nicht akzeptabel. Schon aus den fehlenden Rechtschutzmöglichkeiten europäischer Bürger gegenüber dem Zugriff US-amerikanischer Sicherheitsbehörden auf ihre Daten ergibt sich, dass selbst wenn die US-Regierung den Privacy Shield den Kommissionswünschen entsprechend umsetzen würde, dies derzeit kein mit der DSGVO gleichwertiges Datenschutzniveau begründet.

2. Entscheidungen

2.1 EuGH-Urteil zur datenschutzrechtlichen Verantwortlichkeit bei Facebook-Fanpages

Der rbb verbreitet - wie alle anderen Rundfunkanstalten - seine Angebote zunehmend auch über die sozialen Netzwerke wie Facebook, Instagram und Twitter. Schon in meinem 13. Tätigkeitsbericht (S. 17 ff.) hatte ich darauf hingewiesen, dass diese Drittplattformen der zumeist in den USA angesiedelten Anbieter nicht unseren Europäischen Datenschutzstandards entsprechen. Bei der Nutzung der Drittplattformen findet ein umfangreiches Tracking des Nutzerverhaltens u.a. für Zwecke der Werbung statt. Dabei ist das konkrete Vorgehen völlig intransparent. Die Rundfunkanstalten hatten bislang damit argumentiert, dass sie mit ihren Angeboten auf den sozialen Plattformen nur diejenigen Personen ansprechen, die diese Medien ohnehin bereits nutzten. Außerdem verbreiten sie ihre Inhalte nicht exklusiv auf den sog. „Fanpages" dieser Plattformen, so dass niemand gezwungen sei, diese zu nutzen, um öffentlich-rechtliche Angebote zu erreichen. Auf die Datenschutz-Policy der Anbieter der Drittplattformen hätten sie keinen Einfluss und wiesen in einem Disclaimer auf diesen Umstand hin. Dieses Vorgehen schützt die Rundfunkanstalten jedoch nicht länger:

Am 05.06.2018 hat der Europäische Gerichtshof (EUGH) entschieden, dass die Betreiber von Fanpages auf Facebook gemeinsam mit Facebook für die von Facebook durchgeführte Verarbeitung von personenbezogenen Daten der Nutzer verantwortlich sind. Vorausgegangen war der Entscheidung ein Vorlagebeschluss des Bundesverwaltungsgerichts (BVerwG) vom 25.02.2016. Gegenstand des Verfahrens vor dem BVerwG ist die Frage der Rechtmäßigkeit der Untersagung des Betriebs einer Facebook-Fanpage seitens einer privatrechtlich organisierten Wirtschaftsakademie in Schleswig-Holstein durch die dortige Datenschutzaufsichtsbehörde. Diese war der Meinung, dass die Datenverarbeitung durch Facebook rechtswidrig sei und mo-

nierte außerdem, dass weder die Wirtschaftsakademie noch Facebook die Betroffenen über die Datenverarbeitung hinreichend aufgeklärt hatten.
Nach Feststellung des EuGH erhalten Betreiber von Fanpages über den Dienst „Facebook Insight" anonymisierte statistische Nutzungsdaten der Besucher der Fanpage. Die Datenbasis für diese Statistiken sammelt Facebook über Cookies, die für zwei Jahre auf den Endgeräten der Nutzer gespeichert werden. Betreiber von Fanpages können auf Facebook einstellen, welche Zielgruppen sie primär ansprechen möchten (z. B. nach Alter, Geschlecht, beruflicher Situation, Interessen) und darüber (mit)steuern, wer angesprochen und wessen Daten verarbeitet werden. Nach Auffassung des EuGH begründet diese Steuerungsmöglichkeit die Mitverantwortung des Betreibers, weil er durch die Einstellungen an der Entscheidung über die Zwecke der Verarbeitung beteiligt ist. Allerdings ist dem Betreiber eine vollständige Deaktivierung der Analysefunktion nicht möglich. Das Urteil lässt offen, ob allein die beschriebene Steuerungsfunktion zu der Mitverantwortung des Seitenbetreibers führt, oder ob eine Mitverantwortlichkeit auch dann besteht, wenn keine solche Steuerungsmöglichkeit gegeben ist.

Der EuGH führt weiter aus, dass nicht zwingend eine gleichwertige Verantwortung zwischen Facebook und dem Betreiber der Fanpage bestehen muss, sondern dass der Grad der Verantwortung in verschiedenen Phasen und für verschiedene Verarbeitungen durchaus unterschiedlich sein kann. Aufgrund der gesamtschuldnerischen Haftung gemeinsam Verantwortlicher nach der DSGVO, können jedoch Ansprüche generell gegen jeden der gemeinsam Verantwortlichen geltend gemacht werden, d. h. Betreiber von Fanpages können für die Datensammlung durch Facebook nach der Entscheidung des EuGH in Anspruch genommen werden.

Obwohl das Urteil noch auf Grundlage der EU Datenschutz-Richtlinie von 1995 (Richtlinie 95/46/EG, DS-RL) und nicht auf Grundlage der DSGVO ergangen ist, hat es auch unter Geltung der DSGVO zentrale Bedeutung, da der Begriff des „Verantwortlichen" faktisch unverändert aus der DS-RL in die DSGVO übernommen wurde. Zusätzlich ergibt sich nun Folgendes:

Im Gegensatz zur alten Rechtslage sieht die DSGVO vor, dass gemeinsam Verantwortliche nach Art. 26 DSGVO einen Vertrag zur gemeinsamen Verantwortung schließen und darin u.a. regeln, wer konkrete Pflichten gegenüber den Betroffenen übernimmt (sog. „Joint-Controller-Vertrag"). Weiterhin bestehen für Verantwortliche alle Pflichten nach der DSGVO unmittelbar, so dass die Betreiber von „Fanpages" unter anderem insbesondere die Informationspflichten nach Art. 13, 14 DSGVO gegenüber den Betroffenen erbringen und Auskunftsverlangen von Betroffenen erfüllen müssen.

Im September 2018 stellte die DSK in einem Beschluss fest, dass der Betrieb einer Fanpage, wie von Facebook angeboten, ohne Vereinbarung eines Joint-Controller-Vertrags rechtswidrig sei. Sie wies außerdem darauf hin, dass Fanpage-Betreiberinnen und –Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und diese nachweisen können müssen.
Kurz darauf veröffentlichte Facebook ein sog. „Addendum" (einseitige Erklärung, die sich auf eine gemeinsame Verantwortung bezog). In diesem stellt Facebook zunächst die gemeinsame Verantwortlichkeit klar. Es hält zugleich fest, die primäre Verantwortung gemäß DSGVO für die Verarbeitung der statistischen Daten zu übernehmen und insoweit sämtliche Pflichten aus der DSGVO zu erfüllen. Allerdings fehlen in dem Addendum zum Teil notwendige Inhalte eines Joint-Controller-Vertrages und werden nach der DSGVO geregelte Zuständigkeiten abbedungen.

Am 29.01.2019 haben sich mehrere Mitglieder des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und DLR (AK DSB) mit Vertretern von Facebook in Berlin getroffen und auf den Abschluss eines DSGVO-konformen Joint-Controller-Vertrages gedrungen. Die Vertreter von Facebook vertraten die Auffassung, dass der EuGH in seiner Entscheidung von einer falschen Tatsachengrundlage ausgegangen sei. Die Fanpage-Betreiber erhielten lediglich anonymisierte Daten, auf deren Zusammenstellung sie keinen Einfluss hätten. Aus Sicht von Facebook erschließe sich daher nicht, warum der EuGH hier eine Verantwortlichkeit der Fan-

page-Betreiber angenommen habe. Die Hoffnungen von Facebook liegen derzeit auf dem noch vor dem EuGH laufenden Verfahren zu den sog. „Like-Buttons“. In diesem Verfahren habe der Generalanwalt den Sachverhalt zutreffend eingeordnet. Nach seiner Ansicht sollte die datenschutzrechtliche Verantwortlichkeit des Seitenbetreibers auf die Verarbeitungsvorgänge beschränkt sein, für die er einen tatsächlichen Beitrag zur Datenverarbeitung leiste.

Die Vertreter von Facebook versicherten, dass man durchaus versuche, den Anforderungen des Art. 26 DSGVO gerecht zu werden. Man arbeite bereits an einer zweiten Version des Joint-Controller-Vertrages. Eine Änderung der Bedingungen müsse allerdings weltweit in dutzenden Sprachen abgestimmt werden und sei aufwändig umzusetzen. Facebook stehe in diesem Zusammenhang auch mit der DSK in Kontakt.

Die Entscheidung des EuGH ist in Ihrer Anwendung nicht beschränkt auf den Betrieb von Facebook-Fanpages, vielmehr stellt sie eine Grundsatzentscheidung zum Begriff des Verantwortlichen und zum Anwendungsbereich der gemeinsamen Verantwortung dar.

2.2 EuGH-Urteil zur gemeinsamen datenschutzrechtlichen Verantwortlichkeit in Sachen Zeugen Jehovas

Kurz nach seiner Entscheidung zu den Facebook-Fanpages hat sich der EuGH in seiner Entscheidung vom 10.07.2018 erneut zur gemeinsamen Verantwortlichkeit mehrerer Akteure geäußert. Die ebenfalls noch auf der EU-Datenschutz-Richtlinie beruhende Entscheidung zur Datensammlung durch die Zeugen Jehovas und ihre Mitglieder enthält außerdem wichtige Aussagen zum Anwendungsbereich des EU-Datenschutzrechts.

Der Entscheidung lag eine Entscheidung der Finnischen Datenschutzkommission zugrunde, mit der sie der Gemeinschaft der Zeugen Jehovas verboten hatte, im Rahmen der von ihren Mitgliedern von Tür zu Tür durchgeführten Verkündungstätigkeit personenbezogene Daten zu erheben oder zu verarbeiten, ohne dass bestimmte rechtliche Voraussetzungen für die Verarbeitung solcher Daten eingehalten werden. In der Begründung ihrer Entscheidung vertrat die Datenschutzkommission die Auffassung, dass die Erhebung der personenbezogenen Daten durch die Mitglieder der Gemeinschaft der Zeugen Jehovas eine Datenverarbeitung im Sinne des Datenschutzgesetzes darstelle und diese Gemeinschaft sowie ihre Mitglieder gemeinsam für die Verarbeitung verantwortlich seien.

Der EuGH hat entschieden, dass die Erhebung von personenbezogenen Daten im Rahmen der Verkündigungstätigkeit durch die Zeugen Jehovas datenschutzrechtlich relevant ist und keine Ausübung persönlicher oder familiärer Tätigkeiten darstellt.

Außerdem hat er nochmals bestätigt, dass sich der Begriff „für die Verarbeitung Verantwortlicher“ nicht zwingend auf eine einzige natürliche oder juristische Person beziehe, sondern mehrere an dieser Verarbeitung beteiligte Akteure betreffen könne. Da das Ziel dieser Bestimmung darin bestehe, durch eine weite Definition des Begriffs des „Verantwortlichen“ einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten, habe das Bestehen einer gemeinsamen Verantwortlichkeit nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure für dieselbe Verarbeitung personenbezogener Daten zur Folge. Vielmehr könnten diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein, so dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen sei. Eine gemeinsame Verantwortlichkeit mehrerer Akteure für dieselbe Verarbeitung setze nicht voraus, dass jeder von ihnen Zugang zu den betreffenden personenbezogenen Daten hat. Nach alledem seien die Fragen des vorlegenden Finnischen Gerichts dahingehend

auszulegen, dass eine Religionsgemeinschaft gemeinsam mit ihren als Verkündiger tätigen Mitgliedern als Verantwortliche für die Verarbeitung personenbezogener Daten angesehen werden könne, die durch eine Verkündigungstätigkeit von Tür zu Tür erfolge, wenn diese von dieser Gemeinschaft organisiert und koordiniert werde. Dabei sei es nicht erforderlich, dass die Gemeinschaft Zugriff auf die Daten hat oder ihren Mitgliedern Anleitungen und Anweisungen zur Art und Weise gegeben hat.

Die Regelungen in der DSGVO zur gemeinsamen Verantwortlichkeit und zur Pflicht, in einer Joint-Controller-Vereinbarung in transparenter Form festzulegen, wer welche Verpflichtung trägt, hat für die Rundfunkanstalten insbesondere im Hinblick auf ihre Gemeinschaftseinrichtungen wie dem Zentralen Beitragsservice (ZBS) und dem Informationsverarbeitungszentrum (IVZ) große Bedeutung. Anders als im Verhältnis zu Facebook und anderen Global Playern sind die Zuständigkeiten hier in der Regel klar festgelegt. Dennoch müssen ordnungsgemäße Joint-Controller-Verträge abgeschlossen werden. Der AK DSB hat für diesen Zweck einen Mustervertrag erarbeitet, der nach und nach für alle Gemeinschaftseinrichtungen abgeschlossen werden soll.

2.3 Urteil des EuGH zur Europarechtskonformität des Rundfunkbeitrags

Der EuGH hat mit Urteil vom 13.12.2018 die Europarechtskonformität des Rundfunkbeitrags in Deutschland bestätigt. Ein Einzelrichter am Landgericht Tübingen hatte dem EuGH im Rahmen eines Vorabentscheidungsverfahrens mehrere Fragen zur Vereinbarkeit des Rundfunkbeitrags mit europarechtlichen Regelungen vorgelegt. Der EuGH hat die Vorlagefragen des Landgerichts Tübingen bereits in weiten Teilen für unzulässig erklärt und darüber hinaus festgestellt, dass der Rundfunkbeitrag keine Neubeihilfe darstellt und deshalb auch nicht von der EU-Kommission genehmigt werden musste.

2.4 Bußgeld für Google

Am 21.01.2019 hat das Exekutivorgan der französischen Datenschutzbehörde CNIL Google nach Maßgabe der DSGVO wegen fehlender Transparenz, unklar formulierter Informationen und fehlender gültiger Einwilligung in Bezug auf personalisierte Werbung mit einer Geldstrafe von 50 Millionen Euro belegt. Moniert wurde, dass die von Google beigebrachten Informationen den Nutzern nicht leicht zugänglich seien. Wichtige Informationen wie beispielsweise die Zwecke der Datenverarbeitung, die Dauer der Datenspeicherung oder die Kategorien von personenbezogenen Daten, die zur Werbepersonalisierung verwendet werden, seien unverhältnismäßig stark über verschiedene Dokumente verteilt. Außerdem seien gewisse Informationen weder klar verständlich noch vollständig.

II. Bund

1. Normen

1.1 Bundesdatenschutzgesetz

Das neue Bundesdatenschutzgesetz (BDSG) ist zusammen mit der DSGVO in Kraft getreten (Erstes Datenschutzanpassungsgesetz).

Für den Bereich der Rundfunkanstalten sind folgende Normen relevant:

In § 19 Abs. 1 Satz 4 ist festgehalten, dass eine innerstaatliche Pflicht zur Zusammenarbeit aller deutschen Aufsichtsbehörden besteht. Dies ist Ausfluss von Art. 51 Abs. 2 S. 1 DSGVO, wonach die nationalen Aufsichtsbehörden verpflichtet sind, zwecks Harmonisierung innerhalb der EU einen Beitrag zur einheitlichen Anwendung der Verordnung zu leisten. Auch die nach Art. 85 und 91 eingerichteten spe-

zifischen Aufsichtsbehörden müssen beteiligt werden. Dies sind insbesondere die Rundfunkdatenschutzbeauftragten und die kirchlichen Datenschutzbeauftragten.
Die damalige Bundesdatenschutzbeauftragte Andrea Voßhoff hatte deshalb im Herbst 2017 Vertreter des AK DSB und der Kirchen eingeladen, um das Verfahren zu besprechen; es konnte keine Einigkeit erzielt werden. Auch in einer zweiten Sitzung am 07.12.2018 wurden den spezifischen Aufsichtsbehörden nicht die gleichen Rechte eingeräumt. Seit Januar 2019 ist der Informatiker Ulrich Kelber Bundesdatenschutzbeauftragter. Ein Treffen aller Aufsichtsbehörden ist für Ende Mai 2019 geplant.

1.2 Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die DSGVO

Im September 2018 hat die Bundesregierung den noch im Gesetzgebungsverfahren befindlichen Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die DSGVO beschlossen. Das Gesetz soll weitere bereichsspezifischen Datenschutzregelungen (u. a. das Deutsche-Welle-Gesetz) des Bundes an die unionsrechtlichen Vorgaben anpassen und demnächst in Kraft treten.

1.3 Gesetz zum Schutz von Geschäftsgeheimnissen

Am 21.03.2019 hat der Deutsche Bundestag das Gesetz zum Schutz von Geschäftsgeheimnissen (Geschäftsgeheimnisgesetz) in der vom Rechtsausschuss geänderten Fassung angenommen. Nachdem am 12. 04. 2019 auch der Bundesrat zugestimmt hat, ist es am 26.04.2019 in Kraft getreten.
Das Geschäftsgeheimnisgesetz soll Unternehmen besser vor Spionage durch Wettbewerber schützen. Es setzt die EU-Richtlinie 2016/943 „über den Schutz vertraulichen Know-Hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnis-

se“) um. Bisher waren die Anforderungen an Unternehmen gering, um eine Information als Geschäftsgeheimnis zu schützen. In Zukunft kann sich nur auf ein Geschäftsgeheimnis berufen, wer sein Know-how durch nach außen hin erkennbare Geheimhaltungsmaßnahmen geschützt und ein berechtigtes Interesse an der Geheimhaltung hat. Der Beschlussfassung des Rechtsausschusses war u. a. eine öffentliche Anhörung im Dezember 2018 vorausgegangen, in der die ARD-Generalsekretärin Frau Dr. Pfab als Sachverständige auf die Risiken des ursprünglichen Gesetzesentwurfs für den investigativen Journalismus aufmerksam gemacht hatte. Die Medienvertreter hatten in einem sog. „Medienbündnis“ ihren Bedenken auch in mehreren schriftlichen Stellungnahmen Nachdruck verliehen. Durch die Änderungen ist es gelungen, eine rechtssichere, eindeutigere und praxistauglichere Umsetzung im Interesse der Meinungs- und Informationsfreiheit entsprechend den Vorgaben der EU-Richtlinie zu erreichen. So ist der Begriff des Geschäftsgeheimnisses entsprechend der bisherigen Rechtsprechung auf Informationen beschränkt worden, an deren Geheimhaltung ein berechtigtes Interesse besteht. Außerdem ist klargestellt worden, dass die Verbote zur Erlangung und Verbreitung von Geschäftsgeheimnissen im Bereich der Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit nicht gelten. Damit ist die Gefahr einer Behinderung der Arbeit der Medien gebannt. Ausnahmen enthält das Gesetz daneben auch für sog. „Whistleblower“, wenn diese Informationen veröffentlichen, um rechtswidrige Handlungen, berufliches oder sonstiges Fehlverhalten aufzudecken.

2. Entscheidungen

2.1 Urteil des Bundesverfassungsgerichts zur Verfassungsmäßigkeit des Rundfunkbeitrags

Mit Urteil vom 18.07.2018 hat das Bundesverfassungsgericht (BVerfG) die Verfassungsmäßigkeit des Rundfunkbeitrags grundsätzlich bestätigt. Beim Rundfunkbeitrag handele es sich nicht um eine Steuer, sondern um eine nichtsteuerliche Abgabe, nämlich um einen Beitrag. Der Rundfunkbeitrag werde für die Möglichkeit erho-

ben, das Programm des öffentlich-rechtlichen Rundfunks zu empfangen und diene der funktionsgerechten Finanzausstattung des öffentlich-rechtlichen Rundfunks. Die Anforderungen des allgemeinen Gleichheitsgrundsatzes aus Art. 3 Abs. 1 Grundgesetz (GG) würden durch die Ausgestaltung des Rundfunkbeitrags im privaten Bereich (mit Ausnahme der Beitragspflicht für Zweitwohnungen) eingehalten. Die Beitragspflicht für Betriebsstätten und Kraftfahrzeuge im nicht privaten Bereich verstoße ebenfalls nicht gegen den allgemeinen Gleichheitssatz. Das Gericht beanstandete jedoch, dass Inhaber von Nebenwohnungen den Rundfunkbeitrag doppelt zahlen müssen. Soweit Wohnungsinhaber nach der derzeitigen Regelung für eine Wohnung bereits zur Leistung eines Rundfunkbeitrags herangezogen worden sind, sei der Vorteil bereits abgegolten.

Der Gesetzgeber ist nun aufgefordert, die derzeitigen Regelungen bis zum 30.06. 2020 entsprechend anzupassen. Das BVerfG hat zudem 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.

2.2 Urteil des Bundesgerichtshofs zur Vererbbarkeit von Facebook-Nutzerkonten

Der Bundesgerichtshof (BGH) hat mit Urteil vom 17.05.2018 bezüglich der Frage zum „digitalen Nachlass“ entschieden, dass Erben Zugang zu dem Facebook-Benutzerkonto einer Erblasserin sowie den darin enthaltenen Inhalten gewährt werden muss. Erben haben damit gegen Facebook und andere vergleichbare Plattformen einen Anspruch, die in dem Account vorgehaltenen Kommunikationsinhalte einzusehen. Nach der gesetzgeberischen Wertung gehen auch Rechtspositionen mit höchstpersönlichen Inhalten wie Tagebücher und persönliche Briefe auf die Erben

über. Digitale Inhalte seien ebenso zu behandeln. Der Anspruch auf Zugang zu dem Konto kollidiere auch nicht mit datenschutzrechtlichen Vorgaben. Der BGH hatte zur Entscheidungsfindung die DSGVO anzuwenden und befunden, dass diese dem Zugang der Erben nicht entgegenstehe. Datenschutzrechtliche Belange von Erblassern seien nicht betroffen, da die Verordnung nur lebende Personen schütze.

Mit diesem Urteil zum digitalen Nachlass gleicht der BGH analoge Schriftstücke, (private) E-Mail- und Social-Media Accounts erbrechtlich an. Bedeutung können derartige Sachverhalte in unterschiedlichen Konstellationen auch für den öffentlich-rechtlichen Rundfunk erlangen.

2.3 Entscheidung des Bundeskartellamtes zur Datenverarbeitung bei Facebook

Mit einer Entscheidung vom 07.02.2019 hat das Bundeskartellamt (BKartA) Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen untersagt. Nach seiner Feststellung nehme Facebook in Deutschland eine marktbeherrschende Stellung ein. Diese verhindere, dass Nutzerinnen und Nutzer frei über die Verwendung ihrer Daten bestimmen können. Deshalb müsse Facebook seine Datenverarbeitung anpassen. Nach den Nutzungsbedingungen von Facebook konnten Nutzer das soziale Netzwerk bislang nur unter der Voraussetzung nutzen, dass Facebook auch außerhalb der Facebook-Seite Daten über den Nutzer im Internet oder auf Smartphone-Apps sammelt und dem Facebook-Nutzerkonto zuordnet. Alle auf Facebook selbst, den konzerneigenen Diensten wie z. B. WhatsApp und Instagram sowie den auf Drittwebseiten mit dem „Like-„ oder „Share-Button“ gesammelten Daten konnten mit dem Facebook-Nutzerkonto zusammengeführt werden. Dies ist nach der Entscheidung des BKartA künftig nur noch mit der ausdrücklichen Einwilligung der Nutzer zulässig. Die Nutzung der Facebook-Dienste dürfe nicht von der Einwilligung des Nutzers in diese Art der Datensammlung und Zusammenführung

aus den verschiedenen Quellen abhängig gemacht werden. Die Entscheidung ist noch nicht rechtskräftig. Sofern sie Bestand hat, müsste Facebook die Vorgaben binnen eines Jahres umsetzen. Klar ist aber, dass Facebook sich wehren will. Das Unternehmen kündigte nämlich unmittelbar nach Bekanntwerden der Entscheidung an, Beschwerde dagegen einzulegen.

III. Berlin/Brandenburg

1. 21. Rundfunkänderungsstaatsvertrag

Am 25.05.2018 ist – zeitgleich mit der DSGVO - der 21. Rundfunkänderungsstaatsvertrag (RÄndStV) in Kraft getreten. Ein Schwerpunkt der Neuregelungen betrifft die Verankerung des Medienprivilegs. Das Medienprivileg ist Ausfluss der Medien- und Pressefreiheit des Art. 5 Abs. 1 GG. Mit seiner Neuregelung sind die Landesgesetzgeber dem Auftrag in der DSGVO (Art. 85 Abs. 1) nachgekommen, die Datenverarbeitung von journalistischen Daten auf nationaler Ebene zu regeln.

Ein weiterer Regelungspunkt des 21. RÄndStV ist eine Änderung des Rundfunkstaatsvertrages, wonach Kooperationen des öffentlich-rechtlichen Rundfunks nicht mehr nach einer bloßen „Kann-Vorschrift" möglich sind, sondern ausdrücklich als Bestandteil des Auftrages gelten.

2. 22. Rundfunkänderungsstaatsvertrag

Am 01. 05 2019 ist der 22. RÄndStV in Kraft getreten. Er hat vor allem die zeitgemäße Ausweitung des Telemedienauftrages des öffentlich-rechtlichen Rundfunks zum Gegenstand. Die Kernpunkte der Novellierung betreffen die Herstellung eigenständiger audiovisueller Inhalte für die Online-Verbreitung, das Angebot der Inhalte

auch außerhalb des dafür jeweils eingerichteten Portals, die 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.

3. Berliner Datenschutzgesetz

Im Zuge der europäischen Datenschutzreform wurde auch das Berliner Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz - BlnDSG) neugefasst. Wirksam wurde das BlnDSG mit seiner Veröffentlichung im Gesetz- und Verordnungsblatt des Landes Berlin am 13.06.2018. Es regelt die Voraussetzungen, unter denen die öffentlichen Stellen des Landes Berlin grundsätzlich personenbezogene Daten verarbeiten dürfen.

In § 18 BlnDSG wird – wie auch schon im alten BlnDSG - auf die Vorschriften zum Beschäftigtendatenschutz im BDSG verwiesen. In § 19 wird das Medienprivileg für den gesamten Medienbereich in Berlin geregelt.

Zur datenschutzrechtlichen Kontrollzuständigkeit findet sich für den rbb keine spezielle Regelung, sodass weiterhin der unveränderte § 38 rbb-StV maßgeblich ist. Die Pflicht zur Bestellung einer betrieblichen Datenschutzbeauftragten als Verbindungsstelle zwischen Unternehmen und staatlicher Aufsichtsbehörde für den Verwaltungsbereich ergibt sich für den rbb (wie für alle anderen öffentlichen Stellen in Berlin) jetzt aus § 4 BlnDSG.

C. Datenschutz und Datensicherheit im rbb

I. Neue Regelwerke

1. Dienstanweisung zur Verarbeitung personenbezogener Daten – Datenschutz-Dienstanweisung

Die Datenschutz-Dienstanweisung ergänzt § 31 der Geschäftsordnung (GO) und dient der praktischen Umsetzung der Datenschutzgesetze. Am 24.04.2019 hat die Geschäftsleitung 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 (Anlage 1). Sie gilt seit ihrer Veröffentlichung am 10.05.2019. In ihr wird das neue rbb-Datenschutz-Management mit den Verantwortlichkeiten und Rollen geregelt. Viele Verantwortlichkeiten bestanden auch schon bislang - zum Teil, ohne dass sich die Mitarbeiterinnen und Mitarbeiter dessen bewusst waren. Der Vorteil der neuen Regelungen liegt u. a. darin, dass die Zuständigkeiten nun klar benannt und deutlich gegeneinander abgegrenzt werden. Außerdem sind in der neuen Datenschutz-Dienstanweisung die nach der DSGVO notwendigen Verfahrensschritte bei der Einführung neuer Verarbeitungstätigkeiten geregelt. Dies sind:

- Schutzbedarfsfeststellung,
- Informationssicherheitskonzept,
- Verzeichnis von Verarbeitungstätigkeiten,
- Datenschutzfolgeabschätzung,
- Berechtigungs- und Löschkonzepte sowie
- Grundregeln im Umgang mit Papierdokumenten.

Im Einzelnen:

1.1 Schutzbedarfsfeststellung

Vor Aufnahme eines neuen Verfahrens zur Verarbeitung von personenbezogenen Daten muss das angemessene Schutzniveau für die personenbezogenen Daten festgelegt werden. Zu diesem Zweck führt der Informationssicherheitsbeauftragte unter Beteiligung der Datenschutzbeauftragten mit dem sog. Informationsverantwortlichen (Leiter des zuständigen Fachbereichs) eine Schutzbedarfsfeststellung durch. Zugleich erfolgt die Vorprüfung zur Notwendigkeit einer Datenschutz-Folgenabschätzung. Die Prüfung und Festlegungen erfolgen anhand eines umfangreichen Fragebogens, der im Arbeitskreis der Informationssicherheitsbeauftragten von ARD, ZDF und DLR erarbeitet wurde. Durch die Mitwirkung der Datenschutzbeauftragten an der Festlegung des Schutzniveaus ist sichergestellt, dass durch richtige Weichenstellung dem Recht auf Datenschutz der Betroffenen von vornherein angemessen Rechnung getragen wird.

1.2 Informationssicherheitskonzept

Auf der Grundlage des Ergebnisses der Schutzbedarfsfeststellung erstellt der Informationssicherheitsbeauftragte in Abstimmung mit der Datenschutzbeauftragten ein Informationssicherheitskonzept, in dem die technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit beschrieben sind. Je höher der festgestellte Schutzbedarf der Daten ist, desto aufwändiger müssen die technischen und organisatorischen Maßnahmen sein. Die Maßnahmen müssen regelmäßig auf Aktualität geprüft und ggf. dem veränderten Stand der Technik angepasst werden.

1.3 Verzeichnis von Verarbeitungstätigkeiten

Gemäß Art. 30 DSGVO sind in einem sog. „Verzeichnis von Verarbeitungstätigkeiten“ (VVT) alle wesentlichen Informationen zu den Verarbeitungstätigkeiten mit personenbezogenen Daten eines Unternehmens zusammenzufassen. Betroffen sind sämtliche ganz oder teilweise automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Auch nach alter Rechtslage bestand schon die Pflicht, ein solches Verzeichnis zu führen. Allerdings haben sich die Anforderungen zum Teil geändert. Der rbb hat die DSGVO daher zum Anlass genommen, ein ganz neues VVT aufzubauen.

Der entsprechende Erfassungsbogen wurde im AK DSB gemeinsam erarbeitet. Auf diese Weise ist sichergestellt, dass die Dokumentation der Verarbeitungsvorgänge in allen Rundfunkanstalten einheitlich vorgenommen wird.

Zusätzlich zu den für die einzelnen Verarbeitungsverfahren ausgefüllten Erfassungsbögen werden die entsprechenden Referenzdokumente wie z. B. das Berechtigungs- und das Löschkonzept in das VVT aufgenommen. Das VVT dient als Grundlage für eine strukturierte Datenschutzdokumentation. Außerdem hilft es bei dem Nachweis, dass die Vorgaben aus der DSGVO eingehalten werden (Rechenschaftspflicht). Das VVT stellt somit ein wesentliches Element des Datenschutz-Managements dar und ist auch für den Informationssicherheitsbeauftragten ein wichtiges Arbeitsmittel.

Von dem Vorhaben, eine einheitliche Software zur Führung des VVT für alle Rundfunkanstalten anzuschaffen (ich hatte im 14. Tätigkeitsbericht diesen Plan erwähnt, s. S. 32), sind wir vorerst abgerückt. Zum einen hatten wir erkannt, dass wir zunächst alle Prozesse und Anforderungen klar definieren mussten. Außerdem haben

wir festgestellt, dass es derzeit noch kein Produkt gibt, das unseren konkreten Bedürfnissen optimal entspricht. Wir werden daher zunächst ohne spezielle Software arbeiten und die weiteren Entwicklungen am Markt beobachten.

Gemäß § 31 Abs. 6 GO führt die Datenschutzbeauftragte das VVT. Allerdings sind die Informationsverantwortlichen von sich aus zur Meldung von neuen Verarbeitungsvorgängen und von Änderungen von bestehenden Verarbeitungsvorgängen an die Datenschutzbeauftragte verpflichtet. Der Erfassungsbogen steht in elektronischer Form im Intranet zum Abruf zur Verfügung.

1.4 Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der DSGVO nachgewiesen werden kann (Art. 35 Abs. 1, 7 DSGVO).

1.5 Berechtigungskonzept

Für jedes Verfahren zur Verarbeitung von personenbezogenen Daten müssen in Abhängigkeit von den zu erledigenden Aufgaben die Zugriffsrechte auf personenbezogene Daten für einzelne Benutzer oder Benutzergruppen festgelegt werden. In dem Berechtigungskonzept werden auch alle Prozesse, die die Umsetzung betref-

fen, beschrieben, wie z.B. das Löschen und Erstellen von Nutzern und Passwortrestriktionen.
Die Zugriffsrechte auf IT-Anwendungen und auf Daten in Papierakten sind von der Funktion abhängig, die die Person wahrnimmt (z.B. Anwenderbetreuung, Systemprogrammierung, Systemadministration, Sachbearbeitung). Dabei dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist.

1.6 Löschkonzept

Für jedes Verfahren zur Verarbeitung von personenbezogenen Daten muss der Informationsverantwortliche auch ein Löschkonzept erstellen. Dieses muss den Grundsatz der Speicherbegrenzung umsetzen. Nach dem Wegfall des Zwecks der Datenverarbeitung, spätestens aber nach Ablauf einer etwaigen gesetzlichen Aufbewahrungsfristen ist die Löschung der Daten notwendig. Das Löschkonzept muss bereits zu Beginn der Datenverarbeitung vorliegen. Bei IT-Systemen ist nach Möglichkeit von vorherein eine automatische Löschung zu implementieren.

1.7 Bearbeitung von Auskunftsersuchen

Wie schon die früheren Datenschutzgesetze, sieht auch die DSGVO neben den aktiven Informationspflichten ein Auskunftsrecht vor. Nach Art. 15 Abs. 1 DSGVO kann die betroffene Person von dem für die Datenverarbeitung Verantwortlichen Auskunft darüber verlangen, welche personenbezogenen Daten über sie verarbeitet werden (z. B. Name, Vorname, Anschrift, Geburtsdatum). Außerdem sind bei der Datenauskunft vor allem noch folgende Informationen mitzuteilen:

• Verarbeitungszwecke,
• Kategorien personenbezogener Daten, die verarbeitet werden,
• Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,
• geplante Speicherdauer,
• Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung,
• Beschwerderecht für die betroffene Person bei der Aufsichtsbehörde,
• Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden und
• das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling.

Die Auskunft ist grundsätzlich innerhalb eines Monats zu erteilen.

Schon vor Wirksamwerden der DSGVO lag die Zuständigkeit für die Bearbeitung von Auskunftsersuchen bei der Datenschutzbeauftragten. Die Tatsachen, dass die DSGVO diese Zuständigkeit ausdrücklich dem Verantwortlichen zuweist und überdies nach Wirksamwerden der DSGVO mit einem hohen Anstieg der Auskunftsersuchen zu rechnen war, führten dazu, dass die Frage der Zuständigkeit im Projekt zur Umsetzung der DSGVO neu überdacht wurde. Viel hatte für die Schaffung einer zentralen Stelle zur Bearbeitung sämtlicher Auskunftsersuchen – einschließlich der Anträge auf Informationszugang nach Informationsfreiheitsgesetz und der neuen urheberrechtlichen Auskunftsansprüche - gesprochen. Am Ende hat sich das Projekt dafür entschieden, diese Aufgabe jedenfalls zunächst bei der Datenschutzbeauftragten zu belassen, um zu einem späteren Zeitpunkt erneut zu entscheiden. Dabei können dann die Erfahrungen der anderen Landesrundfunkanstalten einfließen, die die Zuständigkeiten ganz unterschiedlich geregelt haben.
Bei der Bearbeitung von Auskunftsersuchen gilt folgender Prozessablauf:

Diejenigen Auskunftsersuchen, die sich eindeutig auf die Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Einzug des Rundfunkbeitrags beziehen, werden direkt an den ZBS zur Bearbeitung abgegeben. Diese Verfahrens-

weise stützt sich auf eine entsprechende Vereinbarung aller Landesrundfunkanstalten. Im Fall von unspezifischen Auskunftsersuchen und Löschungsbegehren wird in einigen Landesrundfunkanstalten aufgrund entsprechender Erfahrungswerte vermutet, dass sich das Ersuchen auf Beitragsdatenverarbeitung bezieht. Für den rbb wurde entschieden, in einem Zwischenbescheid zunächst um Konkretisierung des Anliegens zu bitten. In vielen Fällen hat sich das Auskunftsersuchen mit dieser Nachfrage dann erledigt. Die Antragsteller melden sich nicht mehr beim rbb. Hierbei handelt es sich vermutlich um Personen, die kein wirkliches Interesse an einer Antwort haben, sondern sich „ein Hobby daraus machen", die neuen Ansprüche nach der DSGVO einmal „auszuprobieren". In allen anderen Fällen des Auskunftsersuchens wird anhand der Angaben des Antragsstellers unter Zuhilfenahme des VVT in den einzelnen Bereichen des rbb ermittelt, ob Daten über den Antragsteller vorhanden sind und auf dieser Grundlage Auskunft erteilt (zu der Statistik der Auskunftsersuchen s. D VII).

2. Dienstanweisung Auftragsverarbeitung

Auftragsverarbeitung liegt vor, wenn eine externe Stelle personenbezogene Daten im Auftrag des rbb und nach dessen Weisung verarbeitet. Gleiches gilt bereits, wenn auch nur die Möglichkeit besteht, dass die externe Stelle in Erfüllung ihres Auftrags von personenbezogenen Daten Kenntnis erhält, ohne dass damit die inhaltliche Verantwortung für die Aufgabe an die externe Stelle übertragen wird (z. B. Wartungsarbeiten, Hosting o.ä.). Dies schließt auch Datenverarbeitung außerhalb von IT-Systemen mit ein (z. B. Aktenvernichtung). Art. 28 DSGVO schreibt vor, dass der Verantwortliche nur Auftragsverarbeiter beauftragt, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der betroffenen Person gewährleistet. In einer

Vereinbarung müssen die Modalitäten der Zusammenarbeit im Einzelnen festgelegt werden.

Auch schon vor der DSGVO gab es eine entsprechende Verpflichtung. Allerdings ist der Katalog, der die in der Vereinbarung zur Auftragsverarbeitung zu regelnden Punkte enthält, in der DSGVO erweitert worden, mit der Folge dass alle Vereinbarungen zur Auftragsverarbeitung erneuert werden müssen. Im Berichtsjahr konnten bereits viele Vereinbarungen aktualisiert werden. Für einen Teil der Vereinbarungen steht die Aktualisierung allerdings noch aus.

Die DSGVO machte auch eine Überarbeitung unserer entsprechenden Dienstanweisung erforderlich. Die neue „Dienstanweisung Auftragsverarbeitung", die die Geschäftsleitung am 24.04.2019 verabschiedet hat, setzt die Anforderungen aus Art. 28 DSGVO um und ersetzt die „Dienstanweisung für Wartungstätigkeiten und Auftragsverarbeitung" aus dem Jahr 2016. Bei der Neuformulierung wurden die Prozesse von der Auftragsvergabe bis hin zur Auftragsabwicklung klarer formuliert. Anlage der Dienstanweisung ist eine Mustervereinbarung zur Auftragsverarbeitung, die im AK DSB erarbeitet wurde und inzwischen im gesamten öffentlich-rechtlichen Rundfunk zur Anwendung kommt. Die Verwendung von gleichlautenden Vereinbarungen ist gerade bei Verhandlungen mit großen Vertragspartnern von Vorteil, die sich nicht ohne weiteres auf die Vorgaben ihrer Vertragspartner einlassen und gern ihre eigenen, oftmals weniger Schutz bietenden Dokumente verwenden.

II. Projekte und Arbeitsgruppen

1. Projekt Umsetzung DSGVO

Anfang 2018 hat die Abteilung Organisation und IT (OUI) im Auftrag der Intendantin unter der Leitung von Britta Böcker ein Organisationsprojekt zur Umsetzung der

DSGVO gestartet (s. dazu auch mein 14. Tätigkeitsbericht, S. 33). Das Projekt war zunächst bis Ende 2018 befristet. Nachdem zum Jahreswechsel noch mehrere wichtige Punkte offen waren, wurde es bis Ende März 2019 verlängert.
An dem Projekt haben der Informationssicherheitsbeauftragte und dessen Mitarbeiter, die Datenschutzbeauftragte, ihr Vertreter und ihr Mitarbeiter sowie Vertreter aus den Direktionen und Mitarbeitervertretungen mitgewirkt. Wir haben die notwendigen Handlungsfelder für den rbb nach Wirksamwerden der DSGVO ermittelt, einen neuen internen Regelungsrahmen erarbeitet und einzelne Maßnahmen bereits konkret umgesetzt. Insgesamt haben 14 sog. „Status-Treffen" in großer Besetzung stattgefunden. In weiteren 11 Terminen hat sich der „harte Kern" des Projektteams (Leitung, Informationssicherheitsbeauftragter und Datenschutzbeauftragte und ihre jeweiligen Mitarbeiter) mit diversen Einzelthemen befasst. Diese betrafen u.a. die Konzeption und notwendigen Prozesse für die Ermittlung des Schutzbedarfs der Daten, das Verfahren bei der Auswahl von technischen und organisatorischen Maßnahmen zur Datensicherheit einschließlich der regelmäßigen Überprüfung, das Verfahren zur Bewertung und Verbesserung der Security-Maßnahmen, Erstellung des VVT, das Verfahren bei der Vergabe von Datenverarbeitung an Externe (Auftragsverarbeitung), das Verfahren für die Bearbeitung von datenschutzrechtlichen Auskunftsersuchen, das Verfahren für die Durchführung der DSFA, das Verfahren bei der Meldung von Datenschutzpannen an die Aufsichtsbehörde und die Optimierung der Workflows bei der Datenerhebung und bei der Löschung von Daten.

Diese Einzelthemen sind in den vom DSGVO-Projekt erarbeiteten Dienstanweisungen zur Verarbeitung personenbezogener Daten (Datenschutz-Dienstanweisung) und für die Auftragsverarbeitung (Dienstanweisung Auftragsdatenverarbeitung geregelt. (s. l.).

Frau Böcker und die Datenschutzbeauftragte haben darüber hinaus zahlreiche Workshops und Einzelgespräche in Bereichen mit einem hohen Aufkommen an personenbezogenen Daten zur Vermittlung der neuen Rechtslage durchgeführt (u.a.,

Online-Koordination, Hauptabteilung (HA) Personal, Mitarbeitervertretungen und Beauftragte, Justitiariat, Serviceredaktion und HA Gebäudemanagement). Alle Einwilligungserklärungen im Online-Bereich (z. B. für das Abonnement eines Newsletters) wurden erneut eingeholt und dokumentiert. Für besondere Bereiche (u.a. Online, HA Personal und Gremien) wurde frühzeitig gemeinsam mit den Informationsverantwortlichen (Leiter der Fachabteilungen) die nach der DSGVO vor jeder Datenerhebung notwendigen „Information der Betroffenen über die Verarbeitung von personenbezogenen Daten (Datenschutzerklärung)“ erarbeitet. Die „Information über die Verarbeitung der Personaldaten“ ist im Intranet veröffentlicht. Jedem neuen Mitarbeiter händigt die HA Personal diese Information individuell aus. Die Versorgungsempfängerinnen und Versorgungsempfänger haben die Datenschutzinformation per Post erhalten.

Außerdem hat die Datenschutzbeauftragte zusammen mit der HA Personal die datenschutzrechtliche Verpflichtungserklärung überarbeitet, die von allen neuen Mitarbeiterinnen und Mitarbeitern vor Beginn ihrer Tätigkeiten beim rbb unterschrieben werden muss.

In zahlreichen Einzelterminen hat die Datenschutzbeauftragte gemeinsam mit den zuständigen Mitarbeitern der Fachabteilungen eine Bestandsaufnahme der Datenverarbeitung durchgeführt und Formulare an die neue Rechtslage angepasst.

2. Jour Fixe IT-Projekte

In regelmäßigen Terminen informiert die OUI die Mitglieder des Personalrats, die Schwerbehindertenvertretung und die Datenschutzbeauftragte in einem informellen Rahmen über geplante und laufende Projekte. Dieser Rahmen ermöglicht es, offen über Ideen und Probleme zu reden und Beteiligungsrechte zu einem mög-

lichst frühen Zeitpunkt zu identifizieren. Im Berichtszeitraum fanden Termine am 23.04. und 26.11.2018 statt.

In dem Termin am 23.04.2018 haben wir uns unter anderem mit der Dispositionssoftware MIRAAN und mit dem ARD-weiten Projekt eines neuen Servicedesks beschäftigt. Geplant ist ein gemeinschaftliches Ticketsystem, wobei der „1st Level Support" durch einen externen Dienstleister und der „2nd Level Support" durch die Rundfunkanstalten selbst erfolgen soll.

In dem Termin am 26.11.2018 ging es unter anderem um das Projekt „Office 365" und den geplanten elektronischen Gehaltsnachweis.

3. Informationssicherheitskreis

Der Informationssicherheitskreis, den der Informationssicherheitsbeauftragte leitet und dessen Mitglied auch die Datenschutzbeauftragte ist, tagte im Berichtszeitraum am 09.04., 25.06. und 27.08.2018 sowie am 18.02.2019. Schwerpunktthema der Sitzung am 09.04.2018 waren die Ergebnisse einer Sicherheitsüberprüfung der Internetpräsenzen des rbb. In der Sitzung am 25.06.2018 hat der Informationssicherheitsbeauftragte die Mitglieder über das Projekt zur Umsetzung der DSGVO informiert. Eine Mitarbeiterin der HA Gebäudemanagement informierte über den Stand des Projekts „Neues Ausweis- und Berechtigungsmanagementsystem" (s. III Ziffer 5). Der Termin am 27.08.2018 diente ausschließlich der Diskussion über den Entwurf der neuen Dienstanweisung Auftragsverarbeitung (s. I Ziffer 2). In der Sitzung am 18.02.2019 erhielt der Kreis aktuelle Statusberichte zum Projekt DSGVO und zum Sicherheitskonzept rbb sowie zu „Office 365" (s. III Ziffer 2). Der Informationssicherheitsbeauftragte informierte die Mitglieder auch darüber, wie er die Online-Redaktion rbb24 am 04.01.2019 dabei unterstützt hat, zu dem Vorgang der Veröffentlichung von massenweisen Daten und Dokumenten deutscher Politiker und Prominenter durch Cyberkriminelle im Internet zu recherchieren, ohne das rbb-

Hausnetzt zu gefährden. Außerdem informierte er über das Vorhaben, spezielle Rechercheplätze für investigative Recherchen einzurichten.

III. IT-Projekte

1. Umstieg auf Windows 10

Schon im 14. Tätigkeitsbericht habe ich über die Migration vom Betriebssystem Windows 7 auf Windows 10 berichtet (S. 35 ff.). Bis zum Ende 2019 wird der rbb die Migration aller Rechner abgeschlossen haben.

Im November 2018 erschreckte eine Meldung über eine Untersuchung im Auftrag des niederländischen Justizministeriums die Öffentlichkeit. Danach sammle und speichere Microsoft in großem Umfang personenbezogene Daten von Office-Nutzern, ohne sie darüber zu informieren. Bereits bei der Einführung von Windows 10 gab es Kritik hinsichtlich der datenschutzrechtlichen Ausgestaltung des Systems. Im Mittelpunkt stand dabei die automatisierte Übermittlung von Nutzerdaten an Microsoft ohne ausreichende Transparenz und Deaktivierungsmöglichkeit. Für Diskussion sorgten hierbei u.a. die sog. „Telemetrie"-Daten (Informationen, die sich aus technischer Sicht mit der Nutzung des Systems beschäftigen, z. B. Absturzberichte, installierte Anwendungen und Details zur Nutzung oder auch der Typ der verwendeten Hardware). Diese Daten gelangen auf US-Server und können somit auch für US-Strafverfolgungsbehörden zugänglich gemacht werden. Inzwischen hat Microsoft nachgebessert und die Datenverarbeitung im Hintergrund zumindest transparenter gemacht.

Die OUI hat für Windows 10 überall dort, wo es aus technischer Sicht vertretbar ist, datenschutzfreundliche Voreinstellungen vorgenommen. Nur waren dies und die Möglichkeit, individuell andere Einstellungen zu wählen, längst nicht allen Kollegin-

nen und Kollegen bekannt. Auf Anregung der Datenschutzbeauftragten hat die OUI daher im März 2019 die Voreinstellungen unter Windows 10 in einer Übersicht zusammengefasst und im Intranet veröffentlicht. In der Übersicht ist auch gekennzeichnet, welche Einstellungen individuell verändert werden können. Diese individuellen Einstellungen werden mit dem persönlichen Profil auf jeden Computer mitgenommen. Zweimal im Jahr gibt es von Microsoft ein Funktionsupdate. Da nicht ausgeschlossen werden kann, dass nach einem Update die individuellen Datenschutz-Einstellungen verloren gehen, werden die Nutzerinnen und Nutzer nun direkt auf den Clients nach größeren Updates durch die OUI informiert und an die Überprüfung ihrer Einstellungen erinnert.

2. MS Office 365 in der Europa-Cloud

Wie berichtet (14. Tätigkeitsbericht S. 35 ff.) hat der rbb am 15.09.2017 einen Probebetrieb mit MS Office 365 gestartet, an dem zunächst Teile der OUI und die Intendanz und inzwischen die gesamte Geschäftsleitung sowie weitere Bereiche des rbb teilnehmen. Der Probebetrieb hat sich bislang auf die Applikationen SharePoint, OneDrive für Business und Office pro Plus-Paket (Word, Excel, PowerPoint, OneNote etc.) fokussiert. Er war zunächst bis August 2018 befristet und wurde zwischenzeitlich bis Ende Februar 2019 verlängert. Seit diesem Zeitpunkt befindet sich der rbb mit dem Personalrat in Verhandlungen über eine erneute Verlängerung und Ausweitung des Probebetriebs. Geplant ist, den Probebetrieb bis zum 31.12.2019 zu verlängern und um Outlook (Mailclient) bzw. Exchange Online (Maildienst) zu erweitern.

MS Office 365 ist eine Kombination aus zahlreichen Cloud-Diensten und bekannten Office-Applikationen. Zwar erfüllt Microsoft einen hohen Sicherheitsstandard für MS Office 365, allerdings behält sich das Unternehmen explizit vor, Daten bei Bedarf (z. B. aus Performance- oder aus Supportgründen) in die USA zu verschieben.

Aus Sicht des AK DSB wird mit dem Umstieg auf MS Office 365 ein Paradigmenwechsel begangen. Im großen Umfang wird die Verarbeitung von Unternehmensdaten und personenbezogenen Daten in die Hände eines Dritten und in die Cloud gegeben (s. dazu auch Stellungnahme des AK DSB zur möglichen Einführung von Office 365 in der Europa-Cloud – Anlage 1 zum 14. Tätigkeitsbericht).

Im Berichtszeitraum hat es mehrere Veröffentlichungen auf Fach-Portalen wie „Heise Online" gegeben, die grundsätzliche Zweifel an der DSGVO-Konformität von Office 365 dokumentiert haben. Diese Zweifel konnten von Microsoft nicht vollends ausgeräumt werden.

Laut Aussage der Projektleitung konnten bislang folgende Erfahrungen im Probebetrieb gesammelt werden:

- Die Fülle an neuen Möglichkeiten und Anwendungen mit Office365 kann zu einer Überforderung und Ablehnung bei den Mitarbeiter*innen führen.

- Die zunächst wichtigste und umfassendste Änderung für die Mitarbeiter*innen ist der Wechsel von Lotus Notes zu Outlook.

- Für das Rollout der neuen Zusammenarbeitsfunktionen sind weitere Tests notwendig.

- Aus technischer Sicht sind die Migration von Lotus Notes nach Outlook sowie die Bereitstellung der Office365-Accounts die komplexesten Vorhaben. Die geringen Projektressourcen fokussieren sich daher zunächst auf dieses Teilprojekt.

Das Projektteam plant alle rbb-Mitarbeiter*innen bis Ende 2019 nach Outlook überführt zu haben.

Angesichts der großen Tragweite, die der Umstieg auf Microsoft 365 für den rbb hat, und auch wegen der Unumkehrbarkeit dieser strategischen Richtungsentscheidung, hat die Datenschutzbeauftragte die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (PWC) am 14.02.2019 mit einer datenschutzrechtlichen Bewertung der bislang vorgelegten Planungskonzepte beauftragt. Die PWC kommt zu dem Ergebnis, dass die Gewährleistung des Datenschutzes bisher nicht mit der notwendigen Präzision geplant wurde und führt dies auch im Einzelnen aus. Vor diesem Hintergrund hat die Datenschutzbeauftragte der Projektleitung mitgeteilt, dass der Verlängerung und Ausweitung des Probebetriebs derzeit nicht zugestimmt werden könne und die Kollegen gebeten, die noch fehlenden Dokumente jetzt zeitnah zu erstellen und die noch bestehende Unklarheiten auszuräumen.

3. SAP Prozessharmonisierung – Projekt „(D)einSAP“

Mitte 2018 haben die ARD-Landesrundfunkanstalten und das DLR eine Kooperationsvereinbarung zur Durchführung und Umsetzung des Projekts „SAP Prozessharmonisierung“ geschlossen. Angestrebt werden innerhalb der rechtlichen Vorgaben (insbesondere Vergabeordnung und abgeleitete Beschaffungsordnungen der Rundfunkanstalten) einheitliche und effiziente betriebswirtschaftliche Geschäftsprozesse in den beteiligten Rundfunkanstalten, die von einer modernen und nachhaltigen SAP-Lösung unterstützt werden, welche von einem zentralen SAP-Steuerer bereitgestellt wird. Das entsprechende Projekt „(D)einSAP“ besteht aus insgesamt 29 Einzelprojekten und wird nach der Projektmanagementsystematik „Prince 2“ durchgeführt. Das Einzelprojekt 4.3 „Informationssicherheit, Datenschutz und Usability“ unter der Leitung der Usability-Beauftragten des rbb Barbara Prasch hat am 30.10.2018 seine Arbeit aufgenommen. An diesem Kick-Off-Termin hat die Datenschutzbeauftragte teilgenommen, da ursprünglich vorgesehen war, dass sie in dem Projekt für das Thema Datenschutz zuständig sein sollte. Nach Diskussion auf der Sitzung des AK DSB am 08./09.11.2018 hat die Datenschutzbeauf-

tragte entschieden, ihre Mitarbeit am Projekt wieder zu beenden. Es ist nicht Aufgabe des betrieblichen Datenschutzbeauftragten, Datenschutzkonzepte zu erarbeiten, denn dies könnte unter Umständen einen Interessenkonflikt nach sich ziehen. Vielmehr obliegt somit die Erarbeitung eines solchen Konzepts den Verantwortlichen. Mittlerweile hat eine Kollegin aus dem rbb mit datenschutzrechtlichen Kenntnissen neben der Leitung zweier weiterer Teilprojekte die Mitarbeit in dem Teilprojekt übernommen.

4. Unified Communication

In dem letzten Tätigkeitsbericht habe ich auch über die testweise Einführung des Kommunikationsdienstes „Unified Communication“ (UC) berichtet (14. Tätigkeitsbericht, S. 40 f.). Zusätzlich zu den Funktionen einer herkömmlichen Telefonanlage, die in unserer Dienstvereinbarung Telekommunikationsanlagenverbund beschrieben sind, bietet der UC-Testbetrieb folgende weitere Leistungsmerkmale:

One number service:
Erreichbarkeit über die persönliche Festnetznummer auch am Smartphone, ohne dass dem rbb Kosten entstehen,
Telefonie:
Auswahl, ob über PC, Smartphone oder klassischem Telefon telefoniert wird,
Telefonkonferenz:
Einfacher Aufbau von Sprachkonferenzen,
Videotelefonie:
Sofern eine Webcam vorhanden ist, kann mit einem einzelnen anderen Teilnehmer eine Videotelefonie geführt werden,
Web Collaboration:
Die eigene PC-Bildschirmoberfläche kann einem anderen UC-Nutzer angezeigt werden,

Instant Messaging:
Chat-Funktionen.

Auf der Grundlage der von der ARGE Rundfunk-Betriebstechnik (RBT) durchgeführten Schutzbedarfsfeststellung und des ebenfalls von der RBT nach BSI-Grundschutz-Standard 100-2 erstellten Informationssicherheitskonzepts konnte seitens des Datenschutzes dem Probebetrieb zugestimmt werden. Der Probebetrieb mit einer Teilnehmeranzahl von 100 Personen war zunächst bis zum 31.12.2018 befristet. Inzwischen wurde er bis zum 30.06.2019 verlängert und auf weitere ca. 100 Personen erweitert. Seit Oktober 2018 nimmt auch die Datenschutzbeauftragte am Probebetrieb teil und testet die neuen Möglichkeiten.

Auf Nachfrage im zuständigen Fachbereich OUI wurde mitgeteilt, dass eine weitere Verlängerung des Probebetriebs um 6 Monate geplant sei. Die OUI wurde vorsorglich darauf hingewiesen, dass eine Zustimmung zu der erneuten Verlängerung davon abhängig sei, ob die nach der Datenschutz-Dienstanweisung erforderlichen Dokumente vorliegen (u. a. ausgefüllter Erfassungsbogen für das VVT und Datenschutz-Information für die Nutzer.)

5. Test- und Probebetrieb des neuen Ausweis- und Berechtigungmanagementsystems

Im Rahmen des Projektes „Sicherheitskonzept“ beabsichtigt der rbb 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 Projektes sollen in den Zugangsbereichen Fernsehzentrum (FSZ) und Haus des Rundfunks (HdR) Personenvereinzelungsanlagen errichtet werden. In Phase zwei soll das Sicherungskonzept für den Standort Potsdam erarbeitet und umgesetzt werden. In Phase drei soll die Innensicherung optimiert werden.

Die derzeit genutzte Hausausweisdatenbank kann die fachlichen Anforderungen, die an die komplexe Zutritts- und Berechtigungsverwaltung gestellt werden, nicht erfüllen. Vor diesem Hintergrund hat der rbb ein professionelles Ausweis- und Berechtigungsmanagementsystem beschafft. Diese Software wird die aktuelle Hausausweisdatenbank ablösen. Sie soll das künftige Tool für die Verwaltung der Personendaten und Zutrittsberechtigungen, die Steuerung der Zugangsanlagen und die Erstellung der neuen elektronischen Hausausweise sein.

Die Verfahren zur Erstellung der Hausausweise und zur Gewährung von Zutritt wurden im Einzelnen mit der Datenschutzbeauftragten abgestimmt. Alle Daten werden nur innerhalb des Ausweis- und Berechtigungsmanagementsystems sowie im Zutrittskontrollsystem verwaltet und verarbeitet. Mit dem Hersteller der Software, der auch die Wartung des Systems übernommen hat, wurde eine Vereinbarung zur Auftragsverarbeitung abgeschlossen. Außerdem hat die Projektleitung gemeinsam mit der Datenschutzbeauftragten ein Hinweispapier zur Datenverarbeitung für die Nutzer des neuen Hausausweises erarbeitet.

Nachdem auch der Informationssicherheitsbeauftragte seine Zustimmung erteilt hatte und alle notwendigen datenschutzrelevanten Dokumente vorlagen, konnte dem Probebetrieb zugestimmt werden. Er hat am 18.04.2019 begonnen und ist bis zum 17.07.2019 geplant.

6. Print at Work

Die Abteilung OUI verantwortet den Betrieb und Support von etwa 1.100 Druckern, Multifunktionsgeräten und Großkopierern an allen Standorten des rbb. Die Geräte sind teils gekauft, teils gemietet. Dabei sind zahlreiche verschiedene Modelle im Einsatz, die aufgrund ihrer Vielfalt an Funktionen und Eigenschaften einen hohen

Aufwand für Service und Support verursachen. Den Mitarbeiterinnen und Mitarbeitern fehlen derzeit aber auch bestimmte Funktionen, die der aktuelle Gerätepark nicht bietet. So wird zunehmend gefordert, von mobilen Endgeräten (iPhone, iPad) zu drucken. Bereits Ende 2017 wurde daher ein Projekt zur Optimierung der Druckerlandschaft ins Leben gerufen. Dies wurde von der Datenschutzbeauftragten seinerzeit sehr begrüßt, weil sie zuvor immer wieder mit Datenschutz- und Datensicherheitsfragen im Zusammenhang mit der Nutzung einzelner Modelle konfrontiert war, was zu einem hohen Arbeitsaufwand geführt hatte. Außerdem wurde seitens des Personalrates und der Datenschutzbeauftragten seit längerem die Möglichkeit des vertraulichen Drucks gefordert. Daran, dass zur Zeit nicht für alle Beschäftigten die Möglichkeit besteht, vertraulich zu drucken, war u. U. der Umstieg auf eine schon seit längerem geplante elektronische Übersendung der Gehaltsabrechnungen gescheitert (s. dazu auch 14. Tätigkeitsbericht, S.47 f.).

In seiner Sitzung am 12.11.2018 hat die Geschäftsleitung die vom Projekt vorgeschlagenen Grundsätze für die Optimierung der Druckerlandschaft beschlossen. Sie hat die OUI damit beauftragt, den Gerätepark insgesamt zu optimieren und damit die Anzahl der vorhandenen Geräte um mindestens 50 Prozent zu reduzieren. Dies bedeutet, dass auf Arbeitsplatzdrucker weitestgehend verzichtet wird. Stattdessen wird die OUI grundsätzlich zentrale Multifunktionsgeräte zum Kopieren und Scannen sowie mit der Möglichkeit des vertraulichen Druckens zur Verfügung stellen. Vom Grundsatz der zentralen Druckerinseln soll es Ausnahmen für besonders sensible Bereiche und Sekretariate (z. B. Geschäftsleitung, Gremien, Personalvertretungen, Datenschutzbeauftragte, Suchtprävention etc.) geben.

Zur Vorbereitung der Maßnahmen hat das Projekt „Print at Work“ eine Richtlinie erarbeitet. Diese regelt, welche Drucksysteme zum Einsatz kommen und beschreibt die Einsatzanforderungen. Ein externer Dienstleister wird die Service- und Supportleistungen übernehmen und die technischen Verbrauchsmaterialien wie Toner und Trommeln liefern. Nachdem der Informationssicherheitsbeauftragte im Herbst 2018 eine Schutzbedarfsfeststellung beim Personalrat und dessen Druckern als

Stelle mit besonders hohem Schutzbedarf durchgeführt hat, konnten diese hohen Anforderungen verallgemeinert und im Sicherheitskonzept berücksichtigt werden. In dem von der RBT erstellten Sicherheitskonzept ist beschrieben, welche Anforderungen der rbb an die Geräte hat. Diese Anforderungen sind in das Leistungsverzeichnis für die EU-Ausschreibung eingeflossen. Frühestens Mitte September 2019 wird feststehen, welche Firma den Zuschlag erhält. Im besten Fall können nach einer Testphase alle Drucker und Multifunktionsgeräte im November und Dezember 2019 ausgetauscht werden.

Aus Datenschutzsicht ist von besonderer Relevanz, wie die Möglichkeit eines vertraulichen Drucks konkret realisiert wird. Außerdem sind u. a. noch die Dokumentation von Ausdrucken sowie die vorgesehenen Löschfristen zu klären. Für die Mitarbeiter muss eine Datenschutzinformation gemäß Art. 13 DSGVO erarbeitet werden. Hierzu findet ein Austausch mit dem Projektteam statt.

7. ASPR – Passwort Reset Manager

Im letzten Tätigkeitsbericht wurde über die beabsichtigte Einführung einer „Self-Service-Lösung“ für das Passwort-Management (das Zurücksetzen der Passwörter) berichtet. Angedacht war eine Web-Anwendung, die auf Standardkomponenten basiert. Nach einer datenschutzrechtlichen Vorabkontrolle hatte die Datenschutzbeauftragte dem Probebetrieb innerhalb der OUI ab Dezember 2017 zugestimmt.

Inzwischen ist das Projekt gestoppt. Mit der Einführung von Office 365 (s. Ziffer 2) hofft die OUI, eine nutzerfreundlichere Lösung zu erreichen.

8. Neues Fuhrparkmanagementsystem

Im 14. Tätigkeitsbericht wurde außerdem über den geplanten Probebetrieb eines neuen Fuhrparkmanagementsystems berichtet (S. 46). Die Aufnahme des Probebetriebs hat sich aus personellen und planerischen Gründen weiter verzögert.

9. Neues Materialdispositionssystem

Auch wurde im 14. Tätigkeitsbericht von dem Test eines neuen Materialdispositionssystems in der Audioproduktion berichtet (S. 46). Der Test wurde inzwischen abgeschlossen und das System für gut befunden. Weitere Schritte sind der Datenschutzbeauftragten nicht bekannt. Offenbar ist ein Probebetrieb noch nicht in Aussicht genommen.

10. eBanf mobile – Zustimmung Probebetrieb

Die elektronische Bestellanforderung „eBanf" ist eine eigenentwickelte SAP-Anwendung, mit der die Erfassung, Bearbeitung und Genehmigung von Bestellanforderungen im SAP-System möglich ist. Geplant ist zusätzlich zu der Möglichkeit, das System am Arbeitsplatz-PC zu nutzen, über eine Web-Anwendung auch das mobile Arbeiten via Smartphone oder Tablet zu realisieren. Entwickelt wurde die Web-Anwendung „eBanf mobile", die auf der SAP Fiori Technologie beruht und den Genehmigungsprozess der eBanf Anwendung abbildet. Für die Mitarbeiter sollen genau die Bestellanforderungen angezeigt werden, die sie zu prüfen bzw. zu genehmigen haben. Die „eBanf mobile" App soll nur auf rbb eigenen IOS-Geräten zugelassen werden. Die Installation der App erfolgt über das jeweilige Mobile Device Management bzw. kann diese aus dem rbb-App-Store geladen werden. Nachdem

der Informationssicherheitsbeauftragte mit seinem Informationssicherheitskonzept den Probebetrieb freigegeben hat, konnte auch von Seiten des Datenschutzes dem Probebetrieb zugestimmt werden. Wie aus dem Fachbereich zu hören war, ist die Produktiveinführung allerdings aufgrund vorrangiger Projekte ins Stocken geraten.

IV. Beschäftigtendatenschutz

1. SAP-Web-Anwendung xSS

Der rbb beabsichtigt, die Lotus Notes-basierte L-Net Anwendung abzulösen und durch eine SAP Web-Anwendung zum An- und Abwesenheitsmanagement (xSS Abwesenheit, Teamkalender, Arbeitszeiterfassung und Beantragung Urlaub und Freizeitausgleich) zu ersetzen. Dabei wird die sog. „Fiori Technologie" zur Anwendung kommen, die eine geräteunabhängige Benutzerschnittstelle zur Verfügung stellt.

Zukünftig sollen alle Beschäftigte, die in einem festen Beschäftigungsverhältnis stehen, ihren Urlaub und Ausgleich aus dem Freizeitkonto über diese Web-Anwendung beantragen. Zusätzlich wird diese Mitarbeitergruppe dann auch Arbeitszeit bzw. zuschlagspflichtige Arbeitstage in dem System abrechnen können. Damit werden die bisher sehr heterogen gestalteten Prozesse zukünftig in einem System (SAP) stattfinden, was die Übertragungsfehleranfälligkeit, aber auch zeitlichen Verzögerungen bezügliche der Aktualität der Daten sehr deutlich reduziert. Das gleiche gilt für den Fehlmeldeprozess. Neu hinzukommen werden die Genehmigung der Arbeitszeiten und deren Abrechnung für die Beschäftigten im disponierten Dienst.

Über eine Schnittstelle zum Dispositionssystem sollen alle Dienstplandaten und tatsächlich abgeleisteten Arbeitszeiten in die Anwendung importiert und dort von den Prüfenden und Genehmigenden freigegeben werden. Durch die Integration in das Modul SAP-HCM (Personalwirtschaft) werden die Daten zukünftig somit in einem System erfasst, berechnet, genehmigt und können dort jederzeit von den Mitarbeiterinnen und Mitarbeitern eingesehen werden.

Schon am 26.10.2017 hat in meinem Beisein die Schutzbedarfsfeststellung stattgefunden. Erwartungsgemäß hat der stellvertretende Personalchef Herr Nicolas Bielefeld den Schutzbedarf hinsichtlich der Vertraulichkeit und Integrität der Daten als hoch eingeschätzt. Nur für die Verfügbarkeit wurde ein normaler Schutzbedarf festgestellt. Auf dieser Basis hat der Informationssicherheitsbeauftragte am 09.01.2019 eine Stellungnahme zur Informationssicherheit der geplanten SAP Web-Anwendung verfasst. Er hat darauf verwiesen, dass die sog. Fiori-Landschaft bereits für das Verfahren eBanf Mobile vollständig aufgebaut und mit einem Sicherheitskonzept bewertet worden war (s. III Ziffer 10). Der Informationssicherheitsbeauftragte schätzt den Zugriff auf die Anwendungen als sicher ein, da er ausschließlich aus dem gesicherten ARD-CN erfolgen wird. Im ARD-CN läuft ein automatischer Schwachstellen-Scanner, der ständig die verfügbaren Systeme auf bekannte Sicherheitsmängel überprüft und die Administratoren und Informationssicherheitsbeauftragten über die Ergebnisse informiert.

Mit dem Entwicklungspartner der SAP, der die SAP-Standard- Software an die konkreten Bedürfnisse des rbb angepasst hat, und auch die Wartung des Systems übernehmen wird, wurden Vereinbarungen zur Auftragsverarbeitung abgeschlossen. Bei der Konfiguration hat die Datenschutzbeauftragte insbesondere darauf hingewirkt, dass die Aufbewahrungsfristen der Abwesenheitsdaten stärker als bislang begrenzt wurden. Danach sollen Abwesenheiten zukünftig nach sechs Jahren gelöscht werden. In der Anwendung sollen nur die Daten des aktuellen Jahres und des Vorjahres angezeigt werden. Beim Ausfüllen der Erfassungsbögen zum VTT hat die Datenschutzbeauftragte die Projektleiterin unterstützt. Auf der Basis der er-

stellten Dokumente konnte dem Probebetrieb seitens des Datenschutzes zugestimmt werden. Der Start ist inzwischen wegen anderer vorrangiger Projekte auf Herbst 2019 verschoben worden.

2. Neuer Zeugnismanager

Wie berichtet, befindet sich das elektronische Bewerbermanagementsystem Umantis der Firma Haufe beim rbb seit 01.07.2017 im Regelbetrieb (s. 14. Tätigkeitsbericht S. 49 f.) Das Hosting des Systems findet in einem zertifizierten Rechenzentrum in Deutschland statt. Die Datenübertragung und – Speicherung erfolgt verschlüsselt. Nachdem der rbb mit diesem System gute Erfahrung gemacht hat, setzt er seit Anfang 2019 zur Erstellung von Arbeitszeugnissen nun auch den Zeugnismanager der Firma Haufe ein. Auch die in diesem Zusammenhang anfallenden Daten werden in dem externen Rechenzentrum gehostet. Nachdem auch für den Zeugnismanager der entsprechende Erfassungsbogen zum VVT ausgefüllt worden war, konnte der Einführung zugestimmt werden. Allerdings habe ich darauf hingewiesen, dass mit der Firma Haufe sowohl für das Bewerbermanagementsystem als auch für den Zeugnismanager noch aktuelle Vereinbarungen zur Auftragsverarbeitung abzuschließen seien.

3. Anonymes Hinweisgebersystem

Vor dem Hintergrund der „#meetoo-Debatte“ hat der rbb zur Aufklärung und Unterbindung etwaigen sexistischen Verhaltens im Juni 2018 das anonyme Hinweisgebersystem „BKMS“ der Business Keeper AG mit Sitz in Berlin eingeführt. Dabei handelt es sich um eine „Software as a Servive“ (SaaS) mit Datenschutz-Zertifikation. Informationen, die in das Hinweisgebersystem eingegeben werden, werden in einer von der Firma betriebenen Datenbank in einem Hochsicherheitsze-

ntrum gespeichert. Das System kann über das rbb-Intranet und auch über das Internet aufgerufen werden. Die Kommunikation zwischen Client und Server findet mittels einer TLS Verschlüsselung (Transport Layer Security) statt und wird in den Logfiles nicht protokolliert. Ein Rückschluss auf den Hinweisgeber ist somit nicht möglich. Die Meldungen bleiben ausschließlich innerhalb des Hinweisgebersystems. Die Download-Option ist deaktiviert und kann lediglich zur Beweissicherung durch einen Administrator eingeschaltet werden. Das Drucken einer Meldung ist ebenfalls deaktiviert. Dadurch ist sichergestellt, dass nur die Bearbeiter eine Meldung sehen und die Meldungen das System nicht verlassen können.

Die technischen und organisatorischen Maßnahmen zur Einhaltung von Datenschutz und Datensicherheit sind bei diesem System auch aus Sicht unseres Informationssicherheitsbeauftragten vorbildlich. Mit der Business Keeper AG wurde eine Vereinbarung zur Auftragsverarbeitung geschlossen.

Großen Wert haben Personalrat, Informationssicherheitsbeauftragter und die Datenschutzbeauftragte darauf gelegt, dass neben der Sicherheit des Systems an sich auch die internen Abläufe im rbb datenschutzkonform gestaltet wurden. Zu diesem Zweck hat die Datenschutzbeauftragte zahlreiche Gespräche mit den Beteiligten geführt – insbesondere den beiden Kolleginnen und dem Kollegen, die die Hinweise bearbeiten. Dabei handelt es sich um die Frauenvertreterin Frau Lydia Lange, der Konfliktberaterin Frau Christiane Fackeldey und um den stellvertretenden Datenschutzbeauftragten Herrn Axel Kauffmann. Durch die gemeinsam erarbeitete ausführliche Datenschutzinformation ist die notwendige Transparenz hergestellt. Der Aufwand hat sich gelohnt. Die intensive Diskussion im Vorfeld hat aus Sicht des Datenschutzes auch erheblich zur Akzeptanz unter den Beschäftigten geführt. Glücklicherweise scheint es im rbb offenbar kaum nennenswerte Vorkommnisse zu geben. Laut der Frauenvertreterin sind seit der Einführung lediglich vier Meldungen eingegangen. Drei Fälle sind abgeschlossen. Ein Fall ist noch in Bearbeitung.

4. Datenschutz bei gesundheitsfördernden Maßnahmen

Seit einiger Zeit unternimmt der rbb große Anstrengungen, um den Mitarbeiterinnen und Mitarbeitern möglichst attraktive Angebote zur Erhaltung ihrer Gesundheit unterbreiten zu können. Neben den vielfältigen Sport- und Entspannungs-Angeboten der Sportgemeinschaft RBB e.V. finden Maßnahmen in Kooperation mit externen Firmen statt. Außerdem gibt es vergünstigte Mitarbeiterkonditionen bei Fitness-Studio-Anbietern u. ä..
Auch in den Fällen, in denen die Beschäftigten nicht mit dem rbb, sondern mit der rechtlich selbständigen Sportgemeinschaft oder einem externen Anbieter ein vertragliches Verhältnis eingehen, ist der rbb in einer gewissen Mitverantwortung dafür zu sehen, dass mit den Daten der Beschäftigten korrekt umgegangen wird. Aus diesem Grund hat die Datenschutzbeauftragte zusammen mit dem Informationssicherheitsbeauftragten am 03.09.2018 ein ausführliches Beratungsgespräch mit der Vorsitzenden der Sportgemeinschaft Frau Doris Krönig zu den datenschutzrechtlichen Anforderungen an die Verwaltung der personenbezogenen Daten der Kursteilnehmerinnen und –teilnehmer und Trainerinnen und Trainer geführt.

In den Fällen, in denen externe Kooperationspartner auch die Auswertung von Gesundheitsdaten anbieten, wird insbesondere darauf verwiesen, dass diese Auswertungen nur den Beschäftigten persönlich übergeben werden und die Möglichkeit zum Datenmissbrauch ausgeschlossen ist. Bei externen Angeboten wirkt die Datenschutzbeauftragte zumindest auf eine DSGVO-konforme Datenschutzerklärung hin.

Vor dem Hintergrund der rasanten Entwicklung bei der Auswertung von Gesundheitsdaten und den immer vielfältigeren Möglichkeiten einer Verknüpfbarkeit der Daten ist es erfreulich, dass die für das Gesundheitsmanagement zuständigen Kolleginnen und Kollegen in der HA Personal ein ausgeprägtes Gespür für die Daten-

schutzbelange der Beschäftigten haben und die Datenschutzbeauftragte in alle Überlegungen und Planungen von vornherein mit einbeziehen.

5. Erstellung eines anonymisierten SAP-Berichts zur Auswertung von Krankheitstagen

Ende 2018 wurde von der HA Personal die Frage aufgeworfen, ob es aus datenschutzrechtlicher Sicht Einwände gegen eine Auswertung von Krankentagen bezogen auf unterschiedliche Mitarbeitergruppen wie Geschlecht, Alter und Beschäftigungsart gebe. Da die Darstellung pro Direktion auf Hauptabteilungsebene erfolgt, ist auf Grund der Gruppengröße sichergestellt, dass die Auswertungsinhalte weder personenbezogen noch personenbeziehbar sind. Dieser Auswertung wurde daher „grünes Licht" gegeben. Sie ist allerdings noch nicht abgeschlossen.

6. Gefährdungsbeurteilungen mittels Online-Befragungen

In mehreren Pilotprojekten testet der rbb Gefährdungsbeurteilungen mittels Online-Befragungen. Zur Anwendung kommen dabei zwei verschiedene Methoden. Im Vorfeld wurde die Datenschutzbeauftragte von der HA Personal einbezogen. Die Befragungen bei beiden Methoden erfolgen vollumfänglich anonym und gaben keinen Anlass für Einwände.

7. Falsche Datenübermittlung an das Finanzamt

Der rbb hat im März 2019 falsche personenbezogene Daten an das Finanzamt übermittelt. Ehemalige freie Mitarbeiterinnen und Mitarbeiter wurden fälschlicher-

weise als beim rbb aktuell beschäftigt gemeldet. Insgesamt waren ca. 1.800 Personen betroffen.

Nachdem der Fehler bekannt geworden war, hat die Datenschutzbeauftragte diesen Vorfall – in Abstimmung mit der Intendanz – der Aufsichtsbehörde gemeldet. Die falschen Daten wurden umgehend korrigiert und das Finanzamt informiert. Außerdem hat die HA Personal alle betroffenen Mitarbeiterinnen und Mitarbeiter schriftlich über die falsche Datenübermittlung informiert und um Entschuldigung gebeten.

Inzwischen sind die Ursachen für die Falschmeldung aufgeklärt: Die Erfassungsmaske enthielt eine falsche Voreinstellung. Außerdem waren die technischen Mitarbeiterinnen und Mitarbeiter, die für die Datenübermittlung in diesem Jahr erstmalig zuständig waren, im Vorfeld nur unzulänglich unterwiesen worden. Die Gruppe der betroffenen Personen hätte überdies wohl wesentlich kleiner sein können, wenn für die Daten der ehemaligen Mitarbeiterinnen und Mitarbeiter die gesetzlich vorgeschriebenen Löschfristen eingehalten worden wären.

Für die Zukunft ist sichergestellt, dass ein vergleichbarer Fehler nicht mehr vorkommt. Die vorgeschriebenen Löschfristen werden jetzt konsequent umgesetzt, eine andere Erfassungsmaske wird verwendet und die ausführenden Mitarbeiterinnen und Mitarbeiter werden ausführlich unterwiesen.

8. Mitschnitt von Teamrunden per Audio Datei?

Eine Teamleiterin wandte sich im Februar 2019 mit der Idee an die Datenschutzbeauftragte, Teamrunden künftig per Audiodatei mitzuschneiden. Aufgrund von Schichtdiensten könnten regelmäßig nicht alle Teammitglieder an den Teamrunden teilnehmen. Ein Protokoll sei daher unverzichtbar. Es falle der Teamleiterin aber

schwer, die Sitzung zu leiten und gleichzeitig ein Protokoll zu erstellen. Vor diesem Hintergrund sei die Idee entstanden, die Besprechungsrunden aufzuzeichnen.

Dieser Idee der Teamleiterin wurde aus datenschutzrechtlicher Sicht abgeraten. Der Hintergrund der Empfehlung ist das gesetzlich geschützte Recht am eigenen Wort als Ausfluss des allgemeinen Persönlichkeitsrechts. Aus Sicht des Datenschutzes gehört es grundsätzlich nicht zu den arbeits- bzw. dienstrechtlichen Pflichten der Teammitglieder, Aufzeichnungen ihrer Redebeiträge zu akzeptieren. Denkbar ist allenfalls eine kurzfristige Aufzeichnung als Gedächtnisstütze für die Protokollantin mit anschließender Löschung. Der Teamleiterin konnte vermittelt werden, dass aus Sicht des Datenschutzes ein solcher Mitschnitt auch dazu führen könnte, dass sich die Beteiligten nicht mehr unbefangen äußern und somit die Qualität der Besprechungen insgesamt leiden könnte.

9. Datenschutz bei der Jugend- und Auszubildendenvertretung

Im vergangenen Herbst wurde die Datenschutzbeauftragte von der Jugend- und Auszubildendenvertretung (JAV) mit ihrer Überlegung informiert, einen privaten JAV- Instagram Account ins Leben zu rufen. Instagram ist ein werbefinanzierter Onlinedienst zum Teilen von Fotos und Videos, der zu Facebook gehört. Bislang hatte die JAV durch die Verbreitung von Bildern und Beiträgen auf Facebook bei den Auszubildenden Präsenz gezeigt. Ausschlaggebend für den geplanten Wechsel zu Instagram war die Tatsache, dass so gut wie alle Auszubildenden eher in Instagram als in Facebook aktiv sind.

Im Gespräch mit der JAV wurden daher – wie auch schon seinerzeit vor dem Start der Nutzung von Facebook – die grundsätzlichen datenschutzrechtlichen Bedenken geäußert. Betont wurde insbesondere, dass zumindest darauf geachtet werden müsse, keine sensiblen personenbezogenen Daten über diesen Weg zu verbreiten.

Bei Fotos ist die Einwilligung aller abgebildeten Personen in die Verbreitung auf Instagram einzuholen. Außerdem dürften die Informationen für die Auszubildenden nicht exklusiv auf Instagram verbreitet werden.

V. Datenschutz bei der Produktion und im Programm

1. Datenverarbeitung bei Akkreditierungen

Seit vielen Jahren werden von Veranstaltern politischer, gesellschaftlicher oder sportlicher Großveranstaltungen Akkreditierungen durchgeführt, um einen sicheren und reibungslosen Ablauf zu erreichen. Je nach Gefährdungslage entscheidet der Veranstalter zusammen mit der zuständigen Polizeibehörde über die Frage, ob im Rahmen des Akkreditierungsverfahrens auch eine Zuverlässigkeitsüberprüfung erforderlich ist. Wird dies bejaht, unterstützt die Polizei den Veranstalter dahingehend, dass sie die vom Veranstalter zur Verfügung gestellten Daten der Akkreditierungsbewerber mit polizeilichen ggf. auch nachrichtendienstlichen Systemen abgleicht und ihn über das Ergebnis informiert.

Im Sommer 2018 wandte sich ein Mitglied des Personalrats mit der Frage an mich, ob es datenschutzrechtlich zulässig sei, dass der Bereich Audioproduktion von Mitarbeiterinnen und Mitarbeitern eine pauschale Einwilligung in die dauerhafte Speicherung ihrer personenbezogenen Daten für Akkreditierungszwecke und in die jeweiligen Datenübermittlungen an die Veranstalter einholt und vor der einzelnen Übermittlung an den Veranstalter nicht noch einmal ausdrücklich um Erlaubnis fragt. Im Gespräch mit dem zuständigen Bereichsleiter hat sich meine Vermutung bestätigt, wonach es nicht im Belieben der Kolleginnen und Kollegen steht, an einzelnen Außenproduktionen teilzunehmen. Es gehört vielmehr zu ihren Dienstpflich-

ten, diese Termine wahrzunehmen, wenn die Kolleginnen und Kollegen entsprechend eingeteilt sind. Die Mitarbeiterinnen und Mitarbeiter müssen daher die Übermittlung ihrer Daten dulden und eine ggf. geforderte Zustimmung zu einer Sicherheitsüberprüfung des Veranstalters erteilen. Diese Pflicht besteht allerdings nur, wenn und soweit die Datenverarbeitung durch den Veranstalter korrekt erfolgt.

Die Datenverarbeitung einschließlich Übermittlung der Daten zu Akkreditierungszwecken erfolgt auf der Grundlage von Art. 6 Abs. 1 b) DSGVO im Rahmen des Dienstvertrages bzw. i. V. m. § 26 Abs. 1 BDSG im Rahmen des Arbeitsvertrags. Auch die dauerhafte Vorhaltung der Daten für diese Zwecke ist aus Sicht des Datenschutzes gerechtfertigt, da es unverhältnismäßig wäre, für ca. 45 Akkreditierungsverfahren pro Jahr immer wieder aufs Neue Daten von den Mitarbeiterinnen und Mitarbeitern einzuholen. Selbstverständlich müssen die Daten sicher aufbewahrt werden und dürfen nur für solche Mitarbeiterinnen und Mitarbeiter zugänglich sein, die mit der Durchführung der Akkreditierungen befasst sind. Mit dem Bereichsleiter wurde verabredet, dass diese Mitarbeiterinnen und Mitarbeiter sich vor einer Datenübermittlung jeweils davon vergewissern müssen, dass die Datenverarbeitung beim Veranstalter korrekt erfolgt. Sollten sie auch nur die geringsten Zweifel an der Rechtmäßigkeit des Verfahrens haben, wird die Datenschutzbeauftragte mit einbezogen. Auf diese Weise ist sichergestellt, dass mit den personenbezogenen Daten der Kolleginnen und Kollegen kein Missbrauch geschieht.

Da – wie ausgeführt – die Datenübermittlung zu Akkreditierungszwecken nicht von der Einwilligung der Betroffenen abhängig ist, sondern sich diese Duldungspflicht unmittelbar aus dem Arbeitsvertrag ergibt, trifft den Bereichsleiter lediglich eine Pflicht zur Datenschutzinformation gemäß Art. 13 DSGVO. Der Text der Information u. a. über die Art und Weise der Datenverarbeitung für die betroffenen Mitarbeiterinnen und Mitarbeiter wurde mit mir abgestimmt und entspricht im Wesentlichen dem Inhalt der Datenschutzinformation der Abteilung Bild, die ihren spezifischen Text bereits zuvor mit mir abgestimmt hatte.

2. OpenMedia/Multimediales Redaktions- und Planungssystem (MRPS)

Das OpenMedia System ist das zentrale Redaktionssystem für Hörfunk, Fernsehen und Online. Mit Hilfe dieses Redaktionssystems werden die komplexen Prozesse des gesamten Beitragszyklus von der Idee bis zum Ausspielen eines Beitrags abgebildet, koordiniert und gesteuert. Das macht OpenMedia zu einem System, auf das nur noch schwer verzichtet werden kann. Ende 2018 hat die RBT im Auftrag des rbb nachträglich ein Informationssicherheitskonzept erstellt. Darin sind die vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) empfohlenen Schutzmaßnahmen sehr ausführlich aufgeführt. Ein Abgleich der Konfiguration des Systems mit den vom BSI empfohlenen Schutzmaßnahmen hat ergeben, dass die Konfiguration alle vom BSI vorgeschlagenen Anforderungen erfüllt.

3. Video Produktions Management System VPMS

Wie in meinem 14. Tätigkeitsbericht erwähnt (S. 39), wird im rbb seit Ende 2016 das Video Produktions Management System VPMS genutzt. Beim Aufbau des VPMS-Systems spielten Datenschutz und Datensicherheit keine Rolle. Erst Ende 2017 hat der Systembetreiber die RBT nachträglich mit der Erstellung eines Sicherheitskonzepts für VPMS beauftragt. Da noch nicht alle darin empfohlenen Maßnahmen umgesetzt worden sind, befindet sich das System nach wie vor im Probebetrieb. Die Umsetzung steht nun aber offenbar kurz vor dem Abschluss.

4. Mobile Reporting

Die Gebrauchsmöglichkeiten von mobilen Telekommunikationsgeräten und die Qualität der Übertragungstechnik entwickeln sich rasant. Der rbb will diese Entwicklung

für Produktionszwecke nutzbar machen. Aus diesem Grund hat er zusätzlich zu der herkömmlichen Produktionsform das Mobile Reporting, d. h. das Produzieren von TV-Beiträgen mit dem Smartphone eingeführt. Reporterinnen und Reporter drehen mit dem Smartphone und schneiden das Material anschließend mit dem Laptop selbst. Dabei geht es unter anderem um ergänzende Bilder zum Dreh, besondere Perspektiven und um Aufnahmen, die mit großer Technik schwierig realisierbar sind. Seit 09/2018 findet Mobile Reporting in der Redaktion des Fernsehmagazins zibb im Probebetrieb statt. Der Probebetrieb war zunächst nur auf ein halbes Jahr angesetzt. Inzwischen wurde er um ein halbes Jahr verlängert und auf alle interessierten Redaktionen ausgeweitet. Für die datenschutzrechtliche Freigabe war ausschlaggebend, dass 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. Auch das Ausleihverfahren wird den Anforderungen an den Datenschutz gerecht.

Den presserechtlichen Anforderungen wird die Ausrüstung der sog. „MoJos" (mobile journalists) ebenfalls gerecht. Sie sind durch rbb-Westen etc. eindeutig als rbb-Mitarbeiter erkennbar (wichtig z. B. für die konkludente Einwilligung in Bildaufnahmen). Bei verdeckten Tonaufnahmen kann die Tonaufzeichnung ausgeschaltet werden.

Da mit den mobilen Geräten nun viele Mitarbeiterinnen und Mitarbeiter arbeiten, die zuvor noch nicht (dienstlich) mit der Herstellung von Videoaufnahmen befasst waren, hatte der Personalrat seine Zustimmung zum Probebetrieb von der Durchführung presserechtlicher Schulungen mit dem Schwerpunkt „Recht am eigenen Bild" abgängig gemacht. Da ich im Justitiariat auch für die Bearbeitung von Presserechtsangelegenheiten zuständig bin, habe ich selbst diese Schulungen durchgeführt. Es fanden 4 Termine statt: Am 12. und 18.12.2018 je ein Termin und am 19.12.2018 zwei weitere Termine. In den Schulungen wurde deutlich, dass einige Kolleginnen und Kollegen verunsichert sind. Sie befürchten eine Übermittlung ihrer

Bewegungsdaten und des Anrufverlaufs an den Gerätehersteller Apple sowie unbemerkte Ton- und Bildaufzeichnungen ihrer eigenen Person durch das Gerät. Ich habe die für die Bereitstellung der Geräte zuständige OUI darum gebeten, die Konfiguration der Geräte transparent zu machen. Gemeinsam sind wir derzeit dabei, konkrete Hinweise zur datenschutzfreundlichen Nutzung der Geräte für die Nutzer zu formulieren. Der Informationssicherheitsbeauftragte hat inzwischen nochmals versichert, dass die Konfiguration der Geräte durch den rbb eine unbemerkte Datenübertragung nicht zulässt.

5. zibb-Messenger

Wie berichtet, verbreitet Inforadio seine Informationen auch über die Messenger-Dienste WhatsApp und Telegram (14. Tätigkeitsbericht, S. 63 f.). Ich sehe die Verbreitung unserer Programme über derartige – nicht DSGVO-konformen - Drittplattformen seit jeher kritisch. Durch die EUGH-Rechtsprechung zur datenschutzrechtlichen Mitverantwortung von Facebook Fanpage-Betreibern hat das Thema weitere Brisanz erlangt, da diese Rechtsprechung wohl auch auf die anderen Drittplattformen übertragen werden muss (B I 2.1).

Während bei Inforadio die Verbreitung des Programms im Mittelpunkt steht, ist zibb im Herbst 2018 noch einen Schritt weitergegangen. Dort ist via WhatsApp und Telegram eine echte Kommunikation in beide Richtungen eingerichtet worden. zibb ist nicht mehr nur Sende-, sondern auch Empfangskanal. Neben bloßen Abstimmungen und Meinungsumfragen ruft zibb auch zur Einsendung von selbst generiertem Content (Bilder, Videos, Kommentare etc.) auf, der auch in das Fernsehprogramm einfließt. Ein deutscher Dienstleister leistet bei diesem Verfahren technische Unterstützung. Nachdem der Informationssicherheitsbeauftragte eine Schutzbedarfsfeststellung durchgeführt und keine Sicherheitsbedenken geäußert hatte, konnte dem Probebetrieb – unter Aufrechterhaltung meiner grundsätzlichen Bedenken –

zugestimmt werden. Dabei habe ich Wert darauf gelegt, dass zumindest dem Grundsatz der Transparenz hinreichend Rechnung getragen wird. Über die Anmeldeseite zum Messenger-Dienst hat der Nutzer auf die mit mir inhaltlich abgestimmte Datenschutzerklärung und die Nutzungsbedingen Zugriff. Für eine wirksame datenschutzrechtliche Einwilligung muss er bei der Registrierung die Datenschutzerklärung per Checkbox akzeptieren.

Der Pilotbetrieb des zibb-Messengers läuft seit 04/2019 und ist bis 12/2019 angesetzt. Laut dem Redaktionsleiter läuft der Probebetrieb bislang problemlos. Datenschutzbeschwerden haben weder die Redaktion noch mich bislang erreicht.

6. Gästelistenmanagement-Tool

Schon im Sommer 2017 haben die Verantwortlichen von Radio Fritz ihre Planungen zum Einsatz eines neuen Gästelistenmanagement-Tools der Datenschutzbeauftragten vorgetragen. Das Tool ist eine Eigenentwicklung und unterstützt Fritz bei der Organisation und Durchführung von Veranstaltungen - insbesondere beim Einladen, Informieren und Erfassen von Gästen. Zuvor erfolgte die Organisation von Veranstaltungen mit Hilfe von Excel-Listen und E-Mails. Am 28.06.2017 fand eine Schutzbedarfsfeststellung durch den Informationssicherheitsbeauftragten statt, an dem neben den Verantwortlichen von Fritz auch der stellvertretende Datenschutzbeauftragte teilnahm. Es 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 Frist von vier Wochen gelöscht.

Der Probebetrieb läuft offenbar seit 2017, ohne dass die für eine abschließende datenschutzrechtliche Bewertung erforderlichen Unterlagen vorliegen. Im Laufe der Zeit erfolgten mehrere sehr ausführliche Gespräche zwischen dem Datenschutz

und den Verantwortlichen von Fritz. Leider konnte die Sache noch immer nicht abgeschlossen werden, da folgende Dokumente fehlen:

- Vollständig ausgefüllter Erfassungsbogen für das VVT,
- Informationssicherheitskonzept,
- Datenschutzerklärung und
- Vereinbarung zur Auftragsverarbeitung mit den jeweils in das Gästelistenmanagement involvierten Agenturen.

7. News-Regie Potsdam

Im Sommer 2018 informierte der Leiter der Abteilung Betrieb den Personalrat und die Freien-Vertretung darüber, dass der rbb beabsichtige, ab 01.09.2018 im Vorspann der Nachrichtensendungen rbb 24 (13.00,16.00 und 17.00 Uhr) eine Regietotale aus der Newsregie zu senden. Alle Kolleginnen und Kollegen aus der Redaktion, der Abteilung Bild und der Abteilung Betrieb sollten per Aushang darüber in Kenntnis gesetzt werden. Der Personalrat bat den Abteilungsleiter, das Vorhaben zunächst mit der Datenschutzbeauftragten abzustimmen. Ich habe ihm erklärt, dass die Veröffentlichung von Bildnissen der Mitarbeiterinnen und Mitarbeiter (wenn auch nur von hinten) von der Einwilligung der Betroffenen abhängig ist. Die Einwilligung muss schriftlich eingeholt werden. Dabei muss der Betroffene auf das Recht des jederzeitigen Widerrufs hingewiesen werden. Gemeinsam mit dem Abteilungsleiter habe ich das Anschreiben an die Mitarbeiterinnen und Mitarbeiter und die entsprechende Einwilligungserklärung entworfen. Bislang erreichten den Datenschutz hierzu keine Beschwerden.

8. 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 Probandinnen und Probanden 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 auch sensible Daten wie z.B. Grad der Schwerhörigkeit u.ä. verarbeitet. Auf Einladung der Abteilung habe ich am 19.06.2019 mit den Kolleginnen und Kollegen ausführlich über Datenschutz bei der Probandenakquise und bei der Durchführung der Tests gesprochen. Im Nachgang wurden die schriftlichen Datenschutzinformationen für die Nutzerinnen und Nutzer überarbeitet.

9. Zulässigkeit des Fotografierens oder Filmens nach Inkrafttreten der DSGVO

Im Zusammenhang mit dem Wirksamwerden der DSGV wandten sich vereinzelt journalistische Kolleginnen und Kollegen an den Datenschutz und erkundigten sich danach, ob für das Filmen oder Fotografieren für journalistische Zwecke jetzt womöglich neue Regeln gelten. Andere erkundigten sich, ob sie es hinnehmen müssten, selbst fotografiert zu werden, was z. B. auf Demonstrationen zunehmend vorkomme.

Für das Fotografieren und Filmen nach Wirksamwerden der DSGVO gilt Folgendes:

Fotos und Filme beinhalten personenbezogene Daten im Sinne von Art. 4 DSGVO, wenn hierauf Personen erkennbar sind. Bei der Herstellung von digitalen Fotos

werden zudem Ort und Zeit erfasst. Solche dynamischen Standortdaten stellen ebenfalls personenbezogene Daten im Sinne der DSGVO dar. Bereits die Erhebung der Daten ist eine erlaubnispflichtige Verarbeitung gemäß Art. 4 Abs. 2 DSGVO. Für die journalistische Arbeit gilt aber gemäß Art. 85 Abs. 2 DSGVO das Medienprivileg. Gemäß § 9 c RStV und § 19 BlnDSG ist die journalistische Arbeit – von der Recherche bis zur Archivierung – von den strengen Anforderungen der DSGVO ausgenommen. Lediglich die Datensicherheit muss auch in diesem Bereich gewährleistet sein. Daraus folgt, dass sich für die journalistische Arbeit durch das Inkrafttreten der DSGVO nichts geändert hat. Nach wie vor gilt hier das durch Rechtsprechung geprägte Presserecht.
Noch nicht abschließend geklärt ist die Frage, inwieweit sich zum Beispiel auch Blogger und Internetseitenbetreiber auf das Medienprivileg berufen können. Dort, wo es nicht gilt, bleibt es bei der Anwendung der DSGVO. Danach ist die Herstellung von Fotos und Videos ohne Einwilligung der betroffenen Person rechtlich zulässig, wenn der Aufnehmende die Aufnahmen nur für seinen persönlichen Gebrauch herstellt. Ist eine Veröffentlichung geplant, muss er daran ein berechtigtes Interesse haben. Ob dies gegeben ist, ist eine Frage des jeweiligen Einzelfalls. Im Ergebnis kann festgehalten werden, dass die DSGVO Personenaufnahmen nicht generell verbietet. Es kommt vielmehr auf den jeweiligen Einzelfall an.

10. Datenschutz in den Produktionsverträgen

Zur Reichweite des Medienprivilegs stellen sich über die Frage des geschützten Personenkreises bzw. der geschützten Tätigkeiten hinaus noch viele weitere Fragen. So haben wir im Kreis der Rundfunkdatenschutzbeauftragten die Frage diskutiert, auf welcher Rechtsgrundlage die Verarbeitung von personenbezogenen Daten im Bereich des Rechtemanagements/Lizenzen erfolgt. Im Zusammenhang mit der Beauftragung von Produktionsverträgen kommt es zu Vertragsschlüssen mit unterschiedlichen Mitwirkenden. Die Daten der Mitwirkenden werden zusammen mit den

wesentlichen Inhalten der Verträge im Lizenzmanagement-System erfasst, um vor der Sendung in einem sog. „Rechte- und Kostenklärungsverfahren“ ermitteln zu können, ob die Rechte an der Produktion gegeben sind und welche Kosten eine Ausstrahlung/Wiederholung auslösen würde. Da das Lizenzmanagement im Zusammenhang mit der journalistischen Arbeit steht, wird vertreten, dass es vom Medienprivileg erfasst ist. Nach einem engeren Verständnis werden Daten nur dann zu journalistischen Zwecken verarbeitet, wenn die Zielrichtung in einer Veröffentlichung besteht. Die Rundfunkdatenschutzbeauftragten waren sich einig, dass jedenfalls die datenschutzrechtlichen Betroffenenrechte wie das Recht auf Auskunft über die gespeicherten Daten oder das Recht auf Korrektur falscher Daten auch beim Lizenzmanagement beachtet werden müssen. Alle Rundfunkanstalten haben ihre Produktionsverträge dementsprechend um Hinweise zum Datenschutz ergänzt.

VI. Sonstiges

1. Datenschutz im Justitiariat, im Bereich Compliance und bei der Datenschutzbeauftragten

Das Justitiariat, die Compliance-Beauftragte Frau Dr. Kerstin Skiba und die Datenschutzbeauftragte verwalten ihre Akten – selbstverständlich getrennt - in dem elektronischen Aktenverwaltungssystem WinRA und in geringerem Umfang zusätzlich auch papiergebunden. Mit dem Hersteller der Software WinRa hat der rbb einen Vertrag über Beratungs- und Supportleistungen abgeschlossen und dementsprechend auch einen Vereinbarung zur Auftragsverarbeitung. Diese Vereinbarung ist im Juli 2018 erneuert und an die DSGVO angepasst worden.

Alle drei Bereiche haben das Wirksamwerden der DSGVO im Mai 2018 zum Anlass genommen, ihre Aktenführung im Sinne des Datenschutzes weiter zu optimieren. So wurden die schon zuvor für die Papierakten festgelegten Vernichtungsfristen konsequent auf die Datenhaltung im WinRa-System übertragen. Auf der Basis einer am 14.11.2018 für alle drei Bereiche nachgeholten Schutzbedarfsfeststellung hat der Informationssicherheitsbeauftragte am 29.03.2019 eine Stellungnahme zur Informationssicherheit abgegeben. Darin hat er weitere Maßnahmen zur Verbesserung des Datenschutzes bei der Papierdatenhaltung empfohlen. Die Umsetzung der Maßnahmen ist noch nicht abgeschlossen.

2. Neues Revisions-Softwaretool

In der Revision wächst der Bedarf nach einem zeitgemäßen IT-gestützten Vorgehen. Insbesondere muss eine transparente und nachvollziehbare Prüfungsplanung, -durchführung und –nachschau gewährleistet werden. Die Revision muss sicherstellen, dass die kritischen Risikobereiche/Prozesse nach den Kriterien der höchsten Eintrittswahrscheinlichkeit eines Schadens und der maximalen Schadenshöhe eindeutig und nachvollziehbar identifiziert, analysiert und abschließend behandelt werden. Die Revision hat sich für die Anschaffung einer Software entschieden, die dabei Unterstützung bietet –insbesondere bei der Berechnung der Risikohöhe und der entsprechenden Risikofaktoren. Die Software soll den Arbeitsalltag erleichtern und zu Einsparungen an Zeit und Selbstverwaltungsaufwendungen führen. Alle Mitarbeiterinnen und Mitarbeiter der Revision sollen mit dem neuen Tool arbeiten. Die Administration des Systems wird durch die Abteilung OuI erfolgen. Da der Softwarehersteller die Schulungen durchführt und auch die Wartung des Systems übernommen hat, wurde eine Vereinbarung zur Auftragsverarbeitung mit ihm abgeschlossen.

Nach Durchführung einer Schutzbedarfsfeststellung und Freigabe der Software durch den Informationssicherheitsbeauftragten sowie der Durchführung einer DSFA aufgrund der zum Teil sehr sensiblen personenbezogenen Daten, die mit dem System verarbeitet werden sollen, konnte der Aufnahme des Probebetriebs in der Zeit von Mitte Februar bis Mitte August 2019 zugestimmt werden. Während des Probebetriebs müssen die Angaben für das VVT vervollständigt und aktualisiert werden. Das betrifft unter anderem die geplante Information der Betroffenen über die Verarbeitung ihrer Daten mit dem System und die technischen und organisatorischen Maßnahmen zur Datensicherheit.

3. Datenschutz in der Gremiengeschäftsstelle

Auch die beiden Kolleginnen der Gremiengeschäftsstelle haben sich nach Wirksamwerden der DSGVO im Mai 2018 an die Datenschutzbeauftragte gewandt. In einem ausführlichen Gespräch am 09.10.2018 wurden die Verarbeitungsvorgänge innerhalb des Rundfunkrates besprochen und darauf aufbauend neue Löschfristen beschlossen. Außerdem wurde der Datenerfassungsbogen für Rundfunkratsmitglieder überarbeitet und an die DSGVO angepasst.

D. Datenschutz beim Rundfunkbeitragseinzug

I. Allgemeines

Für den Einzug der Rundfunkbeiträge betreiben die Landesrundfunkanstalten auf der Grundlage von § 10 Abs. 7 Rundfunkbeitragsstaatsvertrag (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 in der Zeit vom 16.04. bis 18.06.2019 unterzeichnet. Da die Rundfunkanstalten gemeinsam für die Datenverarbeitung beim Rundfunkbeitragseinzug im Sinne von Art. 26 DSGVO verantwortlich sind, muss in Ergänzung zur Verwaltungsvereinbarung noch eine sog. Joint Controller-Vereinbarung über die konkrete Verteilung von Verantwortlichkeiten geschlossen werden. Die Rundfunkdatenschutzbeauftragten haben dafür einen Entwurf erarbeitet, der sich derzeit im Abstimmungsprozess befindet.

Soweit der ZBS für den rbb tätig wird, gelten neben der DSGVO die bereichsspezifischen Datenschutzregelungen des RBStV und 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 Datenschut-

zes 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. Mit Wirkung zum 05.07.2018 ist das Amt der behördlichen Datenschutzbeauftragten von der bisherigen Amtsinhaberin auf Frau Katharina Aye übergegangen. Vor Übernahme der neuen Tätigkeit war Frau Aye im Projekt zur Umsetzung der Anforderungen aus der DSGVO „EUDAGO" eingebunden gewesen. Zu Beginn ihrer Tätigkeit als Datenschutzbeauftragte waren ihr daneben zunächst weitere Aufgaben zugewiesen worden. Es hat sich jedoch schnell herausgestellt, dass sie kapazitätsbedingt vollständig mit datenschutzrechtlichen Themen ausgelastet ist. Seit dem 01.01.2019 ist sie infolgedessen zu 100% als Datenschutzbeauftragte tätig. Mit Wirkung zum 01.01.2019 ist außerdem ihr Mitarbeiter Christian Kruse zum ständigen Stellvertreter der Datenschutzbeauftragten ernannt worden. Durch die Mitgliedschaft von Frau Aye und Herrn Kruse im AK DSB 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. Auf dem Meeting der Unterarbeitsgruppe am 20.06.2019 haben Mitarbeiter des ZBS den Stand der Überarbeitung des Löschkonzepts präsentiert. Am folgenden Tag, dem 21.07.2018, ging es um das zweistufigen Auskunftsverfahren und den Inhalt des Auskunftsschreibens. Am 29.11.2018 haben wir uns gemeinsam mit dem Geschäftsführer Herrn Dr. Stefan Wolf und weiteren Mitarbeitern eingehend mit Einzelfragen im Zusammenhang mit der Joint Controller-Vereinbarung beschäftigt. Die Meetings fanden jeweils beim ZBS in Köln statt.

II. Meldedatenabgleich 2018

Mit dem 15. RÄndStV wurde das Finanzierungssystem des öffentlich-rechtlichen Rundfunks von der geräteabhängigen Zahlungspflicht in eine wohnungsbezogene Beitragspflicht umgewandelt. Im Zusammenhang mit dem Systemwechsel fand auf einer entsprechenden Rechtsgrundlage ein umfassender Meldedatenabgleich statt, der zunächst als einmalige Maßnahme vorgesehen war. Auf diese Weise konnten insbesondere diejenigen Haushalte erfasst werden, die bis dahin ihre Geräte nicht angemeldet oder mangels Empfangsgerät nicht gebührenpflichtig waren. Wie im 14. Tätigkeitsbericht berichtet (S. 70 ff.), wurde mit dem 19. RÄndStV ein weiterer vollständiger Meldedatenabgleich gesetzlich verankert. Es hatte sich zwischenzeitlich gezeigt, dass die Bestandsdaten im System des ZBS in gewissen Fallkonstellationen ihre Aktualität einbüßen, ohne dass der ZBS davon hinreichend Kenntnis erlangt (z. B. Wegzug eines bislang zahlenden Lebenspartners ohne Nennung des in der Wohnung verbleibenden und beitragspflichtigen Lebenspartners). Der zweite komplette Meldedatenabgleich hat das Ziel verfolgt, den durch den ersten Meldedatenabgleich erlangten Datenbestand seiner Qualität nach zu erhalten. Zudem sollte damit die notwendige Datengrundlage geschaffen werden, auf der über die Wirksamkeit des in regelmäßigen Abständen durchgeführten Meldedatenabgleichs zur Erreichung auch langfristiger Beitragsgerechtigkeit und –stabilität im Lichte des Datenschutzes entschieden werden kann. Mit der gesetzlichen Verankerung des zweiten Meldedatenabgleichs haben die Länder zugleich seine Evaluation festgeschrieben (§ 14 Abs. 9 a RBStV).

Die Verfassungsmäßigkeit des Meldedatenabgleichs war Gegenstand mehrerer Gerichtsverfahren und wurde höchstrichterlich bestätigt. So wurde zum ersten Meldedatenabgleich entschieden, dass dieser eine geeignete, erforderliche und verhältnismäßige Maßnahme zur Vermeidung eines Vollzugsdefizits und der Herstellung größerer Beitragsgerechtigkeit dient (u.a. OVG Berlin-Brandenburg, Beschl. v. 6. August 2013, OVG 11 S 23.13). Die Verfassungsmäßigkeit der Folgeregelung in

§ 14 Abs. 9 a RBStV wurde vom Bayerischen Verfassungsgerichtshof (BayVGH) bestätigt. Mit einer Popularklage hatte sich ein Antragsteller dagegen gewandt. Er hatte eine Verletzung des Rechts auf informationelle Selbstbestimmung und daneben einen Verstoß gegen den allgemeinen Gleichheitssatz geltend gemacht. Nachdem der Antragsteller seine Klage zurückgenommen hatte, hat der BayVGH das Verfahren eingestellt. In seiner Kostenentscheidung hat das Gericht ausgeführt, dass eine überschlägige Prüfung ergebe, dass die Klage keine Erfolgsaussichten gehabt hätte. Der Eingriff in das Recht auf informationelle Selbstbestimmung sei verfassungsrechtlich gerechtfertigt. Von einer Gefahr der Abrufbarkeit eines umfassenden Persönlichkeitsprofils könne schon mit Blick auf Art und Umfang der wenigen anzuzeigenden Daten keine Rede sein. Dem Risiko, das aus der Größe der Datensammlung auch im Bereich einer einzelnen Landesrundfunkanstalt entsteht, trage der Rundfunkbeitragsstaatsvertrag mit den bereichsspezifischen Vorschriften über die strikte Zweckbindung der erhobenen Daten und der sie flankierenden Löschungspflichten ausreichend Rechnung.
Das BVerfG hat schließlich mit seinem Urteil vom 18.07.2018 bestätigt, dass die Erhebung des Rundfunkbeitrags verfassungsgemäß ist und dabei auf den jetzt zweimal durchgeführten Meldedatenabgleich gemäß §§ 14 Abs. 9, 9a RBStV Bezug genommen (s. B II 2.1).

Begonnen hat der zweite Meldedatenabgleich am 06.05.2018. Die Einwohnermeldeämter haben zu diesem Stichtag die notwendigen Meldedaten fixiert und sie dann sukzessive bis zum 03.07.218 an den ZBS übermittelt.
Das anschließende Procedere erfolgte analog zum ersten Meldedatenabgleich 2013/2014. Nach dem Abgleich wurden diejenigen Personen vom ZBS angeschrieben, die keiner bereits angemeldeten Wohnung zugeordnet werden konnten. Meldeten diese zurück, dass für ihre Wohnung noch kein Beitrag gezahlt wird, wurden sie angemeldet. Diejenigen Personen, die auf mehrmalige Schreiben des ZBS nicht reagierten, wurden automatisch angemeldet, da der ZBS davon ausgehen musste, dass die betreffende Person seit dem Zeitpunkt des übermittelten Einzugsdatums Inhaber der betreffenden Wohnung sei.

Vorläufiges Ergebnis des zweiten Meldedatenabgleichs:

In rund 3,7 Mio. Fällen konnte der ZBS anhand der übermittelten aktuellen Meldedaten Bestandsdaten von bereits angemeldeten Beitragszahlerinnen und Beitragszahlern im System des ZBS bereinigen. Des Weiteren wurden rund 3,6 Mio. klärungsbedürftige Sachverhalte ermittelt. Unter Zugrundelegung der Erfahrungswerte des ZBS aus dem ersten und den bisherigen Erkenntnissen aus dem zweiten Meldedatenabgleich (Stand Februar 2019) könnten bis zu 370 Tsd. Beitragspflichtige Wohnungen durch den erneuten Meldedatenabgleich hinzukommen.

Auch die Durchführung des zweiten Meldedatenabgleichs erfolgte ohne nennenswerte datenschutzrechtliche Vorkommnisse. Nur in Einzelfällen nahmen die Betroffenen ihr Recht auf Auskunft gem. DSGVO wahr oder bemängelten ihre fehlende Einwilligung zur Übermittlung der Daten. Letztere wurden auf die einschlägige Rechtsgrundlage hingewiesen.

III. Umsetzung der Entscheidung des Bundesverfassungsgerichts zur Befreiungsfähigkeit von Nebenwohnungen

Das BVerfG hat in seiner Entscheidung vom 18.07.2018 zur Verfassungsmäßigkeit der Erhebung des Rundfunkbeitrags (B II 2.1) 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.
Diese Maßgabe warf bei der Umsetzung zahlreiche datenschutzrechtliche Fragen auf. Vordringlich war zu klären, ob im Falle der Befreiung einer Nebenwohnung Daten von Mitbewohnern abgefragt werden dürfen, da diese dann ggf. selbst beitragspflichtig wären. Mangels Rechtsgrundlage haben die Rundfunkdatenschutzbeauftragten eine solche Abfrage als unzulässig angesehen. Eine entsprechende Rechts-

grundlage könnte in der neu zu schaffenden gesetzlichen Regelung aus datenschutzrechtlicher Sicht aber aufgenommen werden.

IV. Neues Löschkonzept beim Zentralen Beitragsservice

Schon im 14. Tätigkeitsbericht (S. 71 ff.) habe ich berichtet, dass der ZBS in Abstimmung mit den Rundfunkdatenschutzbeauftragten ein neues, DSGVO-konformes Löschkonzept erarbeitet. Bis Ostern 2018 wurden in einer ersten Stufe alle nicht mehr benötigten Daten aus der alten Rundfunkgebührenwelt (bis 2012) gelöscht. Wie angekündigt, hat der ZBS den Mitgliedern der Unterarbeitsgruppe Beitragsdatenverarbeitung des AK DSB am 20.06.2018 erste Überlegungen für die zweite Löschstufe unterbreitet. Während es bislang nur ein Löschkonzept für die Historie zum Beitragskonto gibt, soll das neue Löschkonzept auch für die historisierten Datensätze gelten. Die historisierten Daten sind zwar im Archiv vorhanden, jedoch ohne Kenntnis einer Beitragsnummer nicht mehr auffindbar. Wegen der auf unterschiedlichste Weise ausgestalteten technischen Abhängigkeiten der Daten untereinander, stellt sich die Erstellung des Löschkonzepts als äußerst komplexes Thema dar. Durch die notwendigen Maßnahmen zur Umsetzung des Urteils des BVerfG zur Befreiungsfähigkeit von Nebenwohnungen musste der ZBS eine neue Priorisierung der Ressourcen vornehmen und die weitere Arbeit am Löschkonzept zunächst zurückstellen. Der ZBS hat angekündigt, dass das Konzept zum Anfang der zweiten Jahreshälfte 2019 vorliegen wird.

V. Schwärzungen auf Kopien von Leistungsbescheiden

Anfang 2019 hat mich eine Beschwerde über die Berliner Datenschutzbeauftragte erreicht, wonach Belege für den Empfang von Sozialleistungen mit Schwärzungen nicht mehr vom ZBS akzeptiert werden. Der ZBS hatte damit argumentiert, dass es sich um Originalurkunden handele, die nicht verändert werden dürften. Hintergrund

war, dass immer öfter Bescheide eingereicht wurden, aus denen die wesentlichen Informationen nicht mehr erkennbar waren. Ich habe die Angelegenheit mit den Kolleginnen und Kollegen des AK DSB diskutiert. Wir waren einstimmig der Meinung, dass eine Befreiung ausgesprochen werden könne, wenn die wesentlichen Inhalte der Urkunde erkennbar seien. Aus datenschutzrechtlicher Sicht sei eine Schwärzung unproblematisch und aufgrund des Prinzips der Datensparsamkeit auch zu begrüßen. Nachdem auch die Arbeitsgruppe Rundfunkbeitragsrecht, eine Unterarbeitsgruppe der Juristischen Kommission, diese Auffassung vertreten hat, hat der ZBS die geänderten Anforderungen wieder zurückgenommen. In seinen Veröffentlichungen im Internet wird nun deutlich erklärt, welche Daten auf den Leistungsbescheiden nicht geschwärzt werden dürfen.

VI. Auskunft nur mit Teilnehmernummer?

In einer weiteren Beschwerde über die Berliner Datenschutzbeauftragte wurde bemängelt, dass auch bei schriftlichen Auskunftsersuchen zur Beitragsdatenverarbeitung Auskünfte nur unter der Voraussetzung erteilt würden, dass die Beitragsnummer genannt wird. Dazu hat der ZBS klargestellt, dass bei schriftlichen Anfragen die postalische Anschrift ausreicht. Nur im Ausnahmefall und wenn eine direkte Zuordnung nicht möglich ist, wird nach der Beitragsnummer gefragt. Etwas anderes gilt nur für telefonische Auskunftsersuchen. Diese Unterscheidung wird von der Berliner Datenschutzbeauftragten ausdrücklich gebilligt.

VII. Auskunftsersuchen und Eingaben

Die Rundfunkanstalten haben in Beitragsangelegenheiten die Bearbeitung von datenschutzrechtlichen Anfragen und sonstigem Routineschriftwechsel dem ZBS übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter

und von individuellen Anfragen mit besonderer datenschutzrechtlicher Bedeutung haben sie sich selbst vorbehalten.

Bis zum 24.05.2018, dem Wirksamwerden der DSGVO, wurden sämtliche Eingaben Betroffener innerhalb des ZBS ausschließlich durch dessen Datenschutzbeauftragte oder den Datenschutzreferenten (seit 25.05.2019 der stellvertretende Datenschutzbeauftragte) beantwortet.

1. Bearbeitung durch ZBS

Im **Zeitraum vom 01.01. bis 24.05.2018** haben die Datenschutzbeauftragte des ZBS und ihr Mitarbeiter folgende Vorgänge aus dem Sendegebiet des rbb bearbeitet:

Ersuchen von Bürgerinnen und Bürgern um Auskunft über zu ihrer Person gespeicherter Daten:	48 (Vorjahr gesamt 50)
Fragen bezüglich der Herkunft von Daten (z. B. Adressen) bzw. der Berechtigung zur Datenerhebung:	4 (Vorjahr gesamt 12)
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen:	8 (Vorjahr gesamt 8)
Andere, nicht zu den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz:	2 (Vorjahr gesamt 7)
Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von Beitragszahler(n)/innen	8 (Vorjahr gesamt 2)

Anzahl der Vorgänge im Zeitraum
01.01. bis 24.05.2018 insgesamt: **70** (Vorjahr gesamt 79)

Zusammenfassend kann für den Zeitraum bis zum 24.05.2018 festgestellt werden, dass bereits zu diesem Zeitpunkt die Gesamtzahl an datenschutzrechtlichen Eingaben des Vorjahres von Personen aus dem Sendegebiet des rbb nahezu erreicht war. Neben der bevorstehenden Geltung der DSGVO und dem damit zusammenhängenden Medieninteresse hat wohl auch der Umstand dazu beigetragen, dass standardmäßige Auskunftsersuchen über Selbstauskunftsportale an den Beitragsservice gerichtet wurden.

Für die Zeit ab 25.05.2018 wurde vom ZBS ein neuer, zweistufiger Prozess zur Erteilung der Auskunft entwickelt:

In der ersten Stufe der Beauskunftung werden im Wesentlichen die aktuellen Stammdaten zu einem Beitragskonto mitgeteilt. Zugleich wird darauf hingewiesen, dass im Einzelfall weitere Daten vorhanden sein können, die auf weitere Nachfrage zur Verfügung gestellt werden. Die Beauskunftungen der ersten Stufe erfolgen durch ein gesondertes Sachbearbeitungsteam. Daneben besteht die Möglichkeit, eine Datenschutzauskunft elektronisch über das ZBS-Onlineportal abzurufen. Werden nach dieser ersten Beauskunftung weitere Daten angefordert oder handelt es sich um einen schwierigen Einzelfall, erfolgt die Bearbeitung ausschließlich durch die Datenschutzbeauftragte des ZBS und ihren Stellvertreter.

Im Zeitraum vom 25.05. bis zum 31.12.2018 wurden für das Sendegebiet des rbb bearbeitet:

Erstauskunft durch die betriebliche DSB/ Ihren Stellvertreter: 12

Erstauskunft durch Spezialteam: 504

Erweiterte Auskunft durch die betriebliche DSB/ihren Stellvertreter	9
Elektronischer Abruf:	42
Sonstige Schreiben:	14
Anzahl der Vorgänge im Zeitraum 25.05 bis 31.12.2018 insgesamt:	**581**

2. Bearbeitung durch die Datenschutzbeauftragte des rbb

Die rbb-Datenschutzbeauftragte erreichten vom **01.01. bis zum 24.05.2018 lediglich 3 Eingaben bzw. Auskunftsersuchen**. Da diese sich eindeutig auf Beitragsdatenverarbeitung bezogen, wurden sie an den ZBS zur Bearbeitung abgegeben.

Für die Zeit ab dem **25.05.2018 bis 31.12.2018** ergibt sich für die rbb-Datenschutzbeauftragte die folgende Statistik, die den Anstieg der Anträge auf Auskunft nach dem Wirksamwerden der EU-DSGVO verdeutlicht:

Auskunftsersuchen bezogen auf Beitragsdatenverarbeitung:	21
Löschbegehren bezogen auf Beitragsverarbeitung:	1
Unspezifische Auskunftsersuchen:	25
Unspezifische Löschbegehren:	2

Sonstige Schreiben:	3
Anzahl der Vorgänge im Zeitraum 25.05 bis 31.12.2018 insgesamt:	**52**

Zum Vergleich: **In 2017 wurden insgesamt nur 15 Vorgänge** von der rbb-Datenschutzbeauftragten bearbeitet.

Die Auskunftsersuchen und das Löschbegehren, die sich eindeutig auf Beitragsdatenverarbeitung bezogen, wurden direkt an den ZBS zur Bearbeitung abgegeben. Auf die nicht spezifischen Auskunftsersuchen wurde zunächst mit einem standardisierten Zwischenbescheid reagiert und um eine Spezifikation des Begehrens gebeten. Ziel dieses zweistufigen Verfahrens ist es, eine gezielte und datensparsame Recherche innerhalb des rbb zu ermöglichen. Auf den Zwischenbescheid haben lediglich sieben Personen nochmals reagiert. Davon zielten vier Antragsteller auf eine Beauskunftung in Beitragsangelegenheiten und konnten an den ZBS abgegeben werden. Zwei der Antragsteller bestanden auf eine Prüfung aller Bereiche im rbb, die daraufhin veranlasst wurde. Ein Antrag bezog sich auf Daten, die in der Serviceredaktion verarbeitet wurden.

In den sonstigen Schreiben finden sich zwei Vorgänge, bei denen es den Antragstellern um die Löschung von Bildmaterial zu ihrer Person bzw. um das Verbot einer Veröffentlichung von Bildmaterial ging. In beiden Fällen habe ich den Begehren stattgegeben und die Löschung veranlasst bzw. dafür gesorgt, dass das Bildmaterial nicht veröffentlicht wurde. Der dritte Vorgang hatte Fragen zur Kommentarfunktion auf rbb24.de zum Thema. Der Nutzer vermutete eine Datenbank beim rbb, die darin gespeicherte Versender an der Nutzung der Kommentarfunktion hindert. Weiterhin wies er auf Probleme bei der Nutzung der Kommentarfunktion hin, deren Ursache er in den jeweiligen Browsereinstellung zur Ausführung von Javascripten sah. Die Prüfung des Sachverhalts in Zusammenarbeit mit der Redaktionsleitung von rbb24 ergab, dass im rbb keine Datenbank existiert, die die Nutzung der Kom-

mentarfunktion reguliert. Auch Probleme im Zusammenhang mit den Browsereinstellungen konnten nicht bestätigt werden.

Über die Berliner Beauftragte für Datenschutz erreichten die Datenschutzbeauftragte **insgesamt sechs Beschwerden**. In allen sechs Fällen ging es um Fragen zur Datenverarbeitung beim Beitragseinzug.

In einem Fall wurde moniert, dass der ZBS – entgegen einer früheren Praxis - Schwärzungen auf den eingereichten Leistungsbescheiden zur Erlangung einer Befreiung von der Pflicht zur Zahlung des Rundfunkbeitrags nicht mehr akzeptiere. Dieser Beschwerde wurde abgeholfen (s. V.). In einem anderen Fall ging es um das zweistufige Verfahren des ZBS bei der Auskunftserteilung. Beanstandet wurde insbesondere, dass die Fragen zur Herkunft der Daten nicht bereits im ersten Auskunftsschreiben konkret beantwortet werden. Das zweistufige Verfahren ist von den Rundfunkdatenschutzbeauftragten als datenschutzrechtlich zulässig bewertet worden. Hier stehen sich mithin derzeit divergierende Einschätzungen der zuständigen Aufsichtsbehörden gegenüber. Der Vorgang konnte daher noch nicht abgeschlossen werden. Auch in den weiteren Anhörungen bzw. Beschwerden die von der Berliner Beauftragten für Datenschutz und Informationssicherheit an die Datenschutzbeauftragte gerichtet wurden, ging es ausschließlich um Beitragsangelegenheiten (s. auch VI.).

VIII. Projekt EUDAGO pro

Zur Umsetzung der Anforderungen der DSGVO wurde im ZBS in 2017 das Projekt „EUDAGO“ aufgesetzt. Im Rahmen dieses Projekts konnten nicht alle Arbeitspakete abschließend bearbeitet werden. Aus diesem Grund wurde das Nachfolgeprojekt „EUDAGO PRO“ aufgesetzt. Die Arbeiten im Rahmen von „EUDAGO PRO“ dauern noch an. In die Zuständigkeit des Projekts fällt auch die Erarbeitung des Löschkonzepts (s. IV.).

IX. Elektronischer Datenabgleich mit der Bundesagentur für Arbeit

Seit längerem streben die Rundfunkanstalten eine Kooperation mit der Bundesagentur für Arbeit an. Es geht um die Schaffung einer Möglichkeit, dass insbesondere ALG II-Empfänger schon beim Jobcenter auch eine Befreiung von der Beitragspflicht bewirken können und nicht die entsprechende Drittbescheinigung des Jobcenters zusammen mit einem Antrag auf Beitragsbefreiung an den ZBS senden zu müssen. Im Auftrag des HR als federführende Anstalt wurde ein Rechtsgutachten erstellt. Dieses kommt zu dem Ergebnis, dass eine automatisierte Datenübermittlung nicht auf der Grundlage von gesetzlichen Erlaubnistatbeständen erfolgen könne, sondern einer Einwilligung der Betroffenen bedürfe. Für die anschließende Datenverarbeitung durch den ZBS bedürfe es hingegen keiner Einwilligung. Bestandteil des Gutachtens ist auch der Entwurf einer Einwilligungserklärung und eines Informationsblatts. Nachdem die Rundfunkdatenschutzbeauftragten das geplante Vorgehen befürwortet haben, hat der hr Gespräche mit der Bundesanstalt für Arbeit aufgenommen. Diese sind noch nicht abgeschlossen.

Als Übergangslösung kann der Beitragszahler auf der Drittbescheinigung des Jobcenters seine Beitragsnummer eintragen und das Jobcenter übermittelt die Drittbescheinigung an den ZBS. Im Rahmen der geplanten Auswertungen zu diesem Verfahren soll auch geprüft werden, ob das Verfahren auch für die anderen Sozialleistungen mit Befreiungsanspruch geeignet ist.

E. Datenschutz im Informationsverarbeitungszentrum

I. Allgemeines

Beim rbb wird als Gemeinschaftseinrichtung von allen ARD-Anstalten und dem DLR das rechtlich unselbstständige Informationsverarbeitungszentrum (IVZ) betrieben. Beim IVZ werden u.a. alle Personal- und Archivdaten verarbeitet. Eine große Zweigstelle ist beim WDR 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. Ende 2018 ist das IVZ von seinem Standort beim rbb in Berlin auf den rbb-Campus nach Potsdam umgezogen. Der rbb ist weiterhin zuständig für die Infrastruktur der Räumlichkeiten.

Das IVZ hat bislang keinen eigenen betrieblichen Datenschutzbeauftragten bestellt. Zwar ist eine solche Bestellung in einer unselbstständigen Gemeinschaftseinrichtung nicht zwingend gesetzlich vorgeschrieben (eine Ausnahme bildet die gesetzliche Regelung für den ZBS), jedoch fordern die Rundfunkdatenschutzbeauftragten angesichts der Menge der vom IVZ verarbeiteten personenbezogenen Daten seit Längerem einen eigenen betrieblichen Datenschutzbeauftragten für diese Gemeinschaftseinrichtung.

Der Informationssicherheitsbeauftragte des IVZ nimmt seine Aufgaben überwiegend von seinem Homeoffice in Kiel wahrnimmt. Zwar hat Herr Paustian an den Standorten von rbb und WDR jeweils einen Stellvertreter, jedoch entstand hier in den letzten Monaten der Eindruck, dass die Ausübung dieses verantwortungsvollen Amtes von Ferne nicht optimal ist (s. dazu IV.).

Erfreulich ist eine Bescheinigung der Fa. Intertek Certification GmbH vom 31.10.2018, Danach sind die Anforderungen der DSGVO hinsichtlich der „Bereit-

stellung von Software als Dienstleistung für die rundfunkspezifische betriebswirtschaftliche und Mitarbeiter-Verwaltung, Hosting anderer rundfunkspezifischer - sowie allgemeiner IKT-Komponenten – und Anwendungen“ eingehalten.

Einmal jährlich findet beim IVZ das sog. „Jahrestreffen IT-Sicherheit und Datenschutz“ statt. Auf diesem Treffen berichtet der Geschäftsführer über Datenschutzrelevante Themen des zurückliegenden Jahres. Das letzte Jahrestreffen fand am 12.12.2018 statt.

II. Mobiles Arbeiten im IVZ

Durch die Möglichkeiten der Digitalisierung und neuer Technologien, speziell im Bereich der Medien, sind im Arbeitsmarktsegment der Informationstechnik auf Bewerberseite moderne, digitale Arbeitsweisen und große Flexibilität hoch bewertet. Das IVZ befindet sich im stetigen Wettbewerb um hoch qualifizierte und spezialisierte Fachkräfte.

Am 14.01.2019 hat das IVZ daher das zweijährige Pilotprojekt „Mobiles Arbeiten“ beim IVZ gestartet. Es soll dazu dienen, Erfahrungen zu sammeln und zu evaluieren, ob die Form des flexiblen Arbeitens für das IVZ dauerhaft infrage kommt. Da keine Bindung an einen fest eingerichteten Arbeitsplatz außerhalb des Betriebes erfolgt, handelt es sich nicht um Telearbeit i. S. der Arbeitsstättenverordnung. Die Teilnahme an dem Projekt ist den ca. 80 Mitarbeiterinnen und Mitarbeitern, die zuvor am IVZ-Standort in Berlin gearbeitet haben, vorbehalten. Die betroffenen Mitarbeiterinnen und Mitarbeiter stammen aus den Bereichen Technik, Rechenzentrum, SAP-Basis, Anwendungen SAP, Archive, Einzelanwendungen, Leitstand sowie kaufmännische Leitung. Die Teilnahme am Mobilen Arbeiten ist freiwillig. Es besteht weder eine Verpflichtung noch ein Rechtsanspruch auf Mobile Arbeit.

Jeder Teilnehmende 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 im IVZ verboten. Der Grund dafür ist, dass der Zustand der privaten Geräte durch das IVZ nicht überprüft werden kann. Das IVZ würde ein unbekanntes Risiko eingehen, wenn diese eine Verbindung ins IVZ-Netzwerk herstellen würden. Weiterhin ist die Vorgabe, nur Dienstgeräte verwenden zu dürfen, ein Beitrag zur mehr-Faktor-Authentifizierung – ein Faktor ist das bestimmte Gerät, ein weiterer Faktor das Passwort und schließlich der Faktor „RSA-Key".

Für die Nutzung von mobilen Endgeräten gibt es eine spezielle Nutzungsrichtlinie. Allen Mitarbeitern wird bei der Einstellung im Rahmen der Informations-Sicherheitsunterweisung der bindende Charakter der IVZ-Richtlinien erklärt.

Bei Übergabe von Dienstgerätes und RSA-Tokens werden die Mitarbeiter über den Gebrauch unterwiesen und ein Ausgabeschein angelegt.

Die technische, personenungebundene Ausstattung am festen IVZ-Arbeitsplatz bleibt vorerst erhalten. Nach Einführung softwarebasierter IP-Telefonie erhält jede Mitarbeiterin bzw. jeder Mitarbeiter ein Headset und eine Telefonsoftware, welche auf dem Laptop eingerichtet wird. Diese Telefonanbindung hat dieselbe Nummer wie der Telefonanschluss in den Räumlichkeiten der Arbeitsstätte, sodass eine Erreichbarkeit unter derselben Kennung gewährleistet ist. Über die bereits genutzte VPN-Technologie des IVZ erfolgt eine Anbindung an die für die Tätigkeiten benötigten Programme, Laufwerke und Systeme.

Aufgrund der vorbildlichen Regelung der Nutzung von mobilen Endgeräten konnte für das Pilotprojekt eine datenschutzrechtliche Zustimmung erteilt werden.

Die ersten Erfahrungen haben gezeigt, dass das Projekt von den Mitarbeitern gut angenommen wird. Alle Bereiche und ca. 98% der Mitarbeiter nehmen an dem Pi-

lotprojekt teil. Dabei ist die Anzahl der Tage sehr unterschiedlich. Sie variiert zwischen einmal im Monat und konsequent bis zu zwei Tagen in der Woche. Nachbesserungsbedarf besteht noch bei der technischen Ausstattung (Video, Chat, Konferenzräume).

III. Neues Ticketsystem auf Basis der freien Software „OTRS“

Wie im 14. Tätigkeitsbericht erwähnt (S. 74), hat das IVZ seit Herbst 2017 ein neues Ticketsystem auf Basis der freien „Software OTRS“ erprobt, das künftig in der gesamten ARD zur Anwendung kommen soll. Ein Ticketsystem ermöglicht einen formalisierten Vorgang für die Abarbeitung von Anfragen. Folgende Disziplinen werden mit dem Ticketsystem unterstützt:

- Incident Management (Störungsmeldung)
- Problem Management
- Change Management (Änderungsanträge).

Außerdem dient das System automatisch der Dokumentation der durch das IVZ erbrachten Dienstleistungen. Schnittstellen zu anderen, nicht IVZ-internen Systemen, die personenbezogene Daten verwalten, sind nicht vorhanden. Das System wird vom IVZ-Rechenzentrum in Berlin betrieben. Mit der externen Support-Firma wurde eine Vereinbarung über Auftragsverarbeitung abgeschlossen. Das Berechtigungs- und das Löschkonzept des neuen Systems wurden datenschutzrechtlich geprüft und der Erfassungsbogen für das VVT gemeinsam mit dem stellvertretenden Informationssicherheitsbeauftragten ausgefüllt.

Nach erfolgreichem Probebetrieb befindet sich das neue Ticketsystem seit Frühjahr 2018 im Regelbetrieb.

IV. Sicherheitsvorfall beim IVZ

Am 20.02.2019 hat der IVZ-Sicherheitsbeauftragte an alle Rundfunkdatenschutzbeauftragten und Informationssicherheitsbeauftragten einen Sicherheitsvorfall gemeldet. Im Kern ging es darum, dass Unbefugte die neuen Räumlichkeiten des IVZ in dem in Potsdam angemieteten Gebäude betreten hatten. Auf Nachfrage bei der IVZ-Geschäftsleitung und bei der für die Gebäudesicherheit verantwortlichen HA Gebäudemanagement des rbb konnte in Erfahrung gebracht werden, dass es sich um einen Vorfall aus dem Januar während der Umzugsphase des IVZ handelte. Dieser Vorfall war zum Zeitpunkt der Meldung bereits komplett behoben. Die IVZ-internen Aufklärung, warum die Information über das Abstellen des Sicherheitsrisikos den Informationssicherheitsbeauftragten erst während der Eskalation des Sicherheitsvorfalls erreicht hatte, dauert an. Der Vorfall wurde zum Anlass genommen, um den Geschäftsführer des IVZ an seine Pflicht aus § 8 Abs. 7 der Verwaltungsvereinbarung zu erinnern, die Datenschutzbeauftragten unverzüglich über datenschutzrelevante Vorfälle zu informieren.

V. ARD-ZDF-Box

Seit einigen Jahren bietet das IVZ den Mitarbeiterinnen und Mitarbeitern eine sichere Alternative zur DropBox. Die Hauptfunktionalität der ARD-ZDF-Box ist der schnelle und einfache Austausch von Dateien. Dabei lassen sich die Daten direkt mit anderen ARD-ZDF-Box-Nutzern teilen. Kolleginnen und Kollegen, die keinen eigenen Zugang zur ARD-ZDF-Box haben, kann per Link der Zugang eröffnet werden.

Anfang 2019 erfuhr die Datenschutzbeauftragte, dass die ARDZ-ZDF-Box offenbar seit Sommer 2018 neue Features hat. Bislang konnten Dokumente nur im Offline-Modus bearbeitet werden. Der Nutzer musste die offline erstellten Dateien hochladen, teilen, organisieren und zur Bearbeitung wieder herunterladen. Der neue Onli-

ne-Modus bietet nun die Möglichkeit, die Daten direkt in der „Box“ zu bearbeiten. Damit ist das neue Verfahren bezogen auf den Datenfluss sicherer und transparenter.

Im Vorfeld wurde die für das IVZ federführende Datenschutzbeauftragte des rbb entgegen der Absprache mit dem Geschäftsführer des IVZ nicht in das Verfahren einbezogen. Der Geschäftsführung des IVZ erklärte dies damit dass die ARD-ZDF-Box eine Anwendung sei, bei der Auftraggeber nicht eine einzelne Rundfunkanstalt, sondern die ARD als Ganzes sei. Dies ist keine stichhaltige Begründung. Denn gerade auch für solche Fälle wurde ja verabredet, dass die Datenschutzbeauftragte vor Ort in die Planungen einbezogen wird. Alternativ besteht die Möglichkeit, sich an den Vorsitzenden des AK DSB zu wenden.

Da es sich bei der Datenverarbeitung durch das IVZ um eine gemeinsame Datenverarbeitung handelt, bei der alle Rundfunkanstalten Verantwortliche im Sinne des Datenschutzgesetzes sind, muss für das IVZ – wie auch für alle anderen Gemeinschaftseinrichtungen – ein Joint-Controller-Vertrag gemäß Art. 26 DSGVO geschlossen werden. Die Datenschutzbeauftragte wird sich dafür einsetzen, dass darin der Ablauf bei der Neueinführung und bei der Änderung von Verarbeitungstätigkeiten noch klarer als bislang geregelt wird.

F. Datenschutz beim ARD-Hauptstadtstudio

Das ARD-Hauptstadtstudio (HSB) ist eine rechtlich unselbstständige Gemeinschaftseinrichtung der ARD. Der rbb ist als Sitzanstalt Federführer für das HSB. Damit ist die rbb-Datenschutzbeauftragte ebenfalls federführend für diese Einrichtung zuständig.

Im Berichtszeitraum habe ich die Kolleginnen und Kollegen u. a. bei der Anpassung der Datenschutzerklärungen zu HSB-Website und zum HSB-Blog beraten. Beide Angebote sind technisch und organisatorisch voneinander getrennt.

Einmal jährlich findet die gemeinsame Veranstaltung von rbb, Programmdirektion, Erstes Deutsches Fernsehen und des HSB, der sog. ARD-Hauptstadttreff, mit Vertretern aus Politik, Kultur, Wirtschaft und Medien statt. Die Organisation des ARD-Hauptstadttreffs obliegt dem rbb. Für die Durchführung der Veranstaltung und Einladung der Gäste zum ARD-Hauptstadttreff am 23.11.2018 hat der rbb mit einer Agentur zusammengearbeitet. Die mit der Agentur geschlossene Vereinbarung zur Auftragsverarbeitung war wie auch das Verfahren bei der Einladung (E-Mail und Online-Registrierung) im Vorfeld mit der Datenschutzbeauftragten abgestimmt.

G. Informationsmaßnahmen

Neben den zahlreichen Informationsmaßnahmen im Zusammenhang mit der DSGVO führte der Datenschutz im Berichtszeitraum folgende Datenschutzschulungen durch:

Am 06.09.2018 hat die Datenschutzbeauftragte gemeinsam mit dem Informationssicherheitsbeauftragten die neuen Auszubildenden für Datenschutz und Informationssicherheit sensibilisiert.

Am 16.10.2018 hat die Datenschutzbeauftragte gemeinsam mit dem Informationssicherheitsbeauftragten die für Führungskräfte obligatorische Schulung zu Datenschutz und Informationssicherheit durchgeführt.

Zusammen mit dem Informationssicherheitsbeauftragten hat die Datenschutzbeauftragte am 13.11.2018 beim Treffen der rbb-Assistent*innen ein Referat zum Thema Datenschutz und Informationssicherheit gehalten.

Der stellvertretende Datenschutzbeauftragte hat gemeinsam mit jeweils unterschiedlichen Mitarbeiterinnen und Mitarbeitern der OUI im Berichtszeitraum an folgenden Tagen die für SAP-Nutzer obligatorische Datenschutzschulung durchgeführt: 24.05., 03.07., 22.08. und 09.10.2018 sowie 13.02.2019. Die Mitarbeiterinnen und Mitarbeiter des IVZ wurden von ihm am 28.08.18 und am 28.11.2018 und die neue Hauptabteilungsleiterin Mediensysteme und IT Frau Annette Bittmann wurde am 14.01.2019 in den genannten Themengebieten durch Herrn Axel Kauffmann geschult.

Am 26.06.2018 und am 4.12.2018 hat der stellvertretende Datenschutzbeauftragte gemeinsam mit dem Informationssicherheitsbeauftragten einen Teil der am

Probebetrieb von MS Office 365 beteiligten Kolleginnen und Kollegen sowohl des rbb als auch des ARD-Hauptstadtstudios geschult.

Der Schulungsbedarf im Datenschutz wächst immer weiter. Seit Jahren ist die Datenschutzbeauftragte mit der Personalabteilung zum Thema E-Learning im Datenschutz im Gespräch – bislang ohne Erfolg. Nach dem Inkrafttreten der neuen Datenschutz-Dienstanweisung und der Dienstanweisung Auftragsverarbeitung wurde ein weiterer Anlauf unternommen. Nun sieht es so aus, als würde in absehbarer Zeit ein E-Learning-Programm erstellt werden.

H. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten arbeiten im Arbeitskreis der Datenschutzbeauftragten (AK DSB) zusammen. Ein wesentliches Ziel ist es dabei, den Datenschutz bei den gemeinsamen Programmangeboten und beim Beitragseinzug nach möglichst einheitlichen Kriterien – d. h. in der Praxis nach den jeweils höchsten Anforderungen – sicherzustellen. 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 Rundfunkdatenschutzbeauftragten bestand, musste nun in allen Rundfunkanstalten – bis auf SWR und NDR – jeweils ein betrieblicher Datenschutzbeauftragter und eine datenschutzrechtliche Aufsichtsbehörde installiert werden, wobei für die Aufsichtsbehörde Hauptamtlichkeit vorgeschrieben wurde. Sonderfälle bilden nach wie vor die drei Rundfunkanstalten HR, RB und rbb mit der gespaltenen Kontrollzuständigkeit. Für diese drei Rundfunkanstalten hat es keine gesetzliche Neuordnung gegeben (s. A I.).

Im Berichtszeitraum fanden am 19./20.04.2018 in Köln (WDR) und am 08./09.11.2018 in Mainz (ZDF) jeweils reguläre Sitzungen statt. Am 13.06.2018 und 12.02.2019 kamen die Rundfunkdatenschutzbeauftragten zu Sondersitzungen in Bonn (DW) zusammen.

Auf der Sitzung am 19./20.04.2018 haben wir uns unter anderem mit folgenden Themen beschäftigt:

- Umsetzung der DSGVO in den Rundfunkanstalten und im Zentralen Beitragsservice,
- gesetzliche Neuregelung der Datenschutzaufsicht in den Rundfunkanstalten,
- geplante Einführung von MS 365 und

- personalisierte Mediatheken.

Auf der Sondersitzung am 13.06.2018 haben wir zahlreiche Einzelfragen im Zusammenhang mit der Umsetzung der DSGVO behandelt. Die Sondersitzung am 12.02.2019 drehte sich im Wesentlichen um alle Fragen der künftigen Zusammenarbeit im AK DSB nach Wirksamwerden der DSGVO.

Auf der Sitzung am 08./09.11. 2018 ging es u.a. um

- die Neuausrichtung des AK DSB und strukturelle Änderungen durch die gesetzliche Neuordnung der Rundfunkdatenschutzaufsicht und der Bestellung betrieblicher Datenschutzbeauftragter,
- das neue Löschkonzept beim ZBS,
- die geplante Neuregelung der Zweitwohnung und die Verwaltungspraxis bis zur Neuregelung,
- die Durchführung des zweiten vollständigen Meldedatenabgleichs,
- die Umsetzung der DSGVO in den Rundfunkanstalten,
- die Konsequenzen aus dem EuGH-Urteil zu Facebook Fanpages,
- Datenschutz bei der Nutzungsmessung,
- Datenschutz bei Akkreditierungen und um
- die geplante Einführung eines softwaregestützten Nutzungsbeziehungsmanagements.

Zum Vorsitzenden des AK DSB wurde mit Wirkung ab 01.01.2019 der Datenschutzbeauftragte des NDR Herr Dr. Heiko Neuhoff gewählt. Zum Stellvertreter wurde der bisherige Vorsitzende, der Datenschutzbeauftragte des MDR Stephan Schwarze gewählt.

II. Zusammenarbeit der datenschutzrechtlichen Aufsichtsbehörden nach der DSGVO

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. Nach zwei Treffen mit der ehemaligen Bundesdatenschutzbeauftragten Frau Andrea Voßhoff hat es noch keine abschließende Regelung der Zusammenarbeit gegeben. Seit 01.01.2019 ist der Informatiker Herr Ulrich Kelber im Amt. Es bleibt abzuwarten, wie sich unter ihm die Zusammenarbeit der Deutschen Aufsichtsbehörden gestalten wird.

III. Teilnahme an Fortbildungen und Veranstaltungen

Im Berichtszeitraum hat die Datenschutzbeauftragte an folgenden Veranstaltungen teilgenommen:

- 16.05./17.05.2018 19. Datenschutzkongress Euroforum:
  Auf der Agenda standen unterschiedliche Themen rund um die DSGVO.

- 24.05.2018 Veranstaltung des Instituts für Europäisches Medienrecht (EMR) zum Thema „Am Vortag der DSGVO - Justiz und Medien als Beispiele für die Herausforderungen beim Umgang mit dem neuen Recht“:
  Auf dieser Veranstaltung stellten Vertreter von Justiz und Medien die Herausforderungen beim Umgang mit der DSGVO dar. Für den öffentlich-

rechtlichen Rundfunk habe ich in einer Art „Werkstattbericht“ einen Überblick über unsere Umsetzungsmaßnahmen gegeben.

- 14.09.2018 Fachgespräch zum Netzwerkdurchsetzungsgesetz (NetzDG):
  Die Bundestagsfraktion Bündnis 90/Die Grünen hatte zu einer Analyse der ersten Auswirkungen des seit 01.01.2018 geltenden NetzDG in den Deutschen Bundestag geladen. Dieses Gesetz soll den Umgang mit illegalen Online-Inhalten in großen sozialen Netzwerken durch Unternehmen wie Facebook und Google regeln.
- 28.01.2019 Veranstaltung der Datenschutzkonferenz (DSK) zum Thema „Europäischer Datenschutz: Chance oder Risiko? Acht Monate DSGVO – Bilanz und Blick nach vorn“:
  Auf dieser Veranstaltung anlässlich des Europäischen Datenschutztages standen Erfahrungen in der Anwendung der DSGVO im Mittelpunkt.

Sämtliche Veranstaltungen fanden in Berlin statt.

Berlin, Mai 2019

gez. Anke Naujock

Anlage: Datenschutz-Dienstanweisung vom 06.05.2019