13. Tätigkeitsbericht

der Beauftragten für den Datenschutz

des

Rundfunk Berlin-Brandenburg

Berichtszeitraum:

01. April 2015 bis 31. März 2016

Dem Rundfunkrat gemäß § 38 Abs. 7 **rbb**-Staatsvertrag
vorgelegt von
Anke Naujock

Inhaltsverzeichnis

Vorbemerkung

Das zurückliegende Jahr war für die Datenschutzbeauftragte erneut sehr arbeitsintensiv. Das hat verschiedene Gründe:

Das Datenschutzrecht befindet sich – abermals – im Wandel. Auch der **rbb** muss sich auf die Umsetzung der Europäischen Datenschutz-Grundverordnung (DS-GVO) zum Frühjahr 2018 vorbereiten. Schon in zwei Jahren wird es kein Bundes- und keine Landesdatenschutzgesetze mehr geben. Auch viele bereichsspezifische Regelungen wie Regelungen desTelemediengesetzes, das bislang den Datenschutz in den Telemediendiensten regelt, werden entfallen. An ihre Stelle wird die DS-GVO treten, die unmittelbare Wirkung entfaltet. Derzeit bin ich dabei, mir einen Überblick darüber zu verschaffen, was das inhaltlich für den **rbb** bedeutet.

Der **rbb** setzt in zunehmendem Maße auf IT-gestützte Systeme. Das gilt sowohl für den Sendebetrieb, als auch für die übrige Betriebsorganisation. Viele Arbeitsprozesse werden inzwischen elektronisch gesteuert, so dass der reibungslose Ablauf wesentlich von der eingesetzten Informationstechnik und dem dazugehörigen Informationssicherheitskonzept abhängt. In diesem Zusammenhang habe ich im Berichtszeitraum einige zum Teil sehr aufwändige Vorabkontrollen durchgeführt. Die Informationssicherheit hat in letzter Zeit nicht nur unter finanziellen und Image-Gesichtspunkten (Datenverlust oder –verfälschung kann teuer werden und einen Verlust an Glaubwürdigkeit zur Folge haben), sondern auch für den Datenschutz eine immer größere Relevanz erhalten. Der Datenschutz ist nur dann gewährleistet, wenn die Datenverarbeitung sicher ist. Daher bin ich froh, dass der **rbb** seit Juli 2016 einen neuen Informations-Sicherheitsbeauftragten hat, der 100% seiner Arbeitszeit der Informationssicherheit widmen kann. Dies entspricht einer langjährigen Forderung von mir und auch dem Leiter der Stabsabteilung Organisation und IT (OUI), Herrn Kruithof. Es zeichnet sich bereits jetzt ab, dass ich mit dem Informationssicherheitsbeauftragten Herrn Kalisch in Zukunft sehr eng zusammenarbeiten werde. In vielen Fragen bin ich auf seine Expertise angewiesen.

Ein weiterer Faktor, der zu einer deutlichen Steigerung des Arbeitsanfalls geführt hat, ist die wachsende Präsenz des **rbb** im Internet mit eigenen Seiten und vor allem auch auf zahlreichen Drittplattformen. Zu klären waren u. a. Fragen zur rechtlichen Verantwortlichkeit von Datenverarbeitungen. Die Datenschutzerklärungen auf den **rbb**-Seiten mussten überarbeitet und aktualisiert werden und neue Tools (= „Werkzeuge") mussten auf Datenschutzkonformität geprüft werden.

In das Berichtjahr fallen neben der Bestellung des neuen Informationssicherheitsbeauftragten auch weitere wichtige personelle Veränderungen. Seit Mai 2016 ist ein neuer Personalrat im Amt. Ich bin gespannt, wie sich die Zusammenarbeit mit diesem für den Beschäftigtendatenschutz wichtigen Gremium entwickeln wird.

Und auch der Wechsel im Amt des Berliner Beauftragten für Datenschutz – seit Januar 2016 ist Frau Maja Smoltczyk im Amt – wird Auswirkungen auf den **rbb** haben. Die Berliner Datenschutzbeauftragte ist zusammen mit der Brandenburgischen Datenschutzbeauftragten Dagmar Hartge oberste Kontrollinstanz für die Datenverarbeitung im wirtschaftlich-administrativen Bereich.

Datenschutz ist wie das Bohren dicker Bretter. Das habe ich in den zurückliegenden Jahren gelernt. Nach vier (!) Jahren Abstimmungsarbeit ist seit Mai 2016 die von mir in Zusammenarbeit mit den Kollegen aus der OUI erarbeitete neue Dienstanweisung für Wartungstätigkeiten und Auftragsdatenverarbeitung endlich in Kraft. Dieser Durchbruch gibt mir den Ansporn, auch in anderen datenschutzrechtlichen Themen, die im **rbb** aus unterschiedlichen Gründen kontrovers diskutiert werden, am Ball zu bleiben. Dabei werde ich von meinem Kollegen aus der Revision, dem stellvertretenden behördlichen Datenschutzbeauftragten des **rbb**, Herrn Axel Kauffmann, tatkräftig unterstützt. Die Zusammenarbeit mit Herrn Kauffmann ist eine große Bereicherung, da er zu vielen Themen neue Aspekte und Perspektiven einbringt. Ihm gilt mein besonderer Dank. Auch meiner Kollegin im Sekretariat, Frau Anja Hubert, möchte ich herzlich für ihre Unterstützung danken.

Förmliche Beanstandungen musste ich im Berichtsjahr nicht aussprechen. Soweit es in Einzelfällen zu Verletzungen der Datenschutzbestimmungen gekommen ist, wurde meinen Empfehlungen in den Fachbereichen umgehend gefolgt.

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 für die Datenschutzbeauftragte des **rbb** haben sich im Berichtszeitraum nicht verändert.

Gemäß § 38 Abs. 1 **rbb**-Staatsvertrag 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 literarischen Zwecken verarbeitet.

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

Für die Sicherstellung des Datenschutzes im wirtschaftlich-administrativen Bereich ist beim **rbb** außerdem – wie bei allen Berliner Behörden und sonstigen öffentlich-rechtlichen Stellen – eine behördliche/ein behördlicher Datenschutzbeauftragte/r sowie jeweils eine Stellvertreterin/ein Stellvertreter schriftlich zu bestellen (§ 36 Abs. 1 **rbb**-Staatsvertrag i. V. m. § 19 a Berliner Datenschutzgesetz – BlnDSG).

Die/der Rundfunkdatenschutzbeauftragte ist eine eigenständige Kontrollstelle im Sinne von Artikel 28 EG-Datenschutzrichtlinie.

II. Konkrete Situation

Auf seiner Sitzung am 3. September 2015 hat mich der Rundfunkrat gemäß § 38 Abs. 1 **rbb**-Staatsvertrag auf Vorschlag der Intendantin für eine weitere Amtszeit von vier Jahren rückwirkend vom 1. Juli 2015 bis zum 30. Juni 2019 zur Beauftragten für den Datenschutz des **rbb** bestellt. Parallel dazu hat die Intendantin für den gleichen Zeitraum meine Bestellung zur behördlichen Datenschutzbeauftragten im Sinne von §19 a BlnDSG entsprechend verlängert. Meine Funktion als Datenschutzbeauftragte des **rbb** nehme ich nebenamtlich zu meiner Tätigkeit im Justitiariat wahr. Seit 1. April 2014 ist der Mitarbeiter der Revision, Herr Axel Kauffmann, stellvertretender behördlicher Datenschutzbeauftragter. Herr Kauffmann vertritt mich in Abwesenheitsfällen. Bei größeren Projekten beziehe ich Herrn Kauffmann von Anfang an mit ein, damit er jederzeit in der Lage ist, im Bedarfsfall für mich einzuspringen. Im Berichtszeitraum hat Herr Kauffmann auch eine Reihe von Datenschutzschulungen übernommen (s. E.).

Für alle Fragen rund um die Informationssicherheit war im Berichtszeitraum bis zum 30. Juni 2016 der Bereichsleiter IT-Betrieb und Systemverantwortliche für Informationssicherheit im **rbb**, Herr Gerry Wolff, verantwortlich.

Seit dem 1. Juli 2016 hat Herr Michael Kalisch die Aufgabe des Informationssicherheitsbeauftragten beim **rbb** übernommen. Positiv ist hervorzuheben, dass sich Herr Kalisch im Unterschied zu seinem Vorgänger zu 100% seiner Arbeitszeit dem Thema Informationssicherheit widmen kann. Bedauerlich finde ich, dass die Funktion des Informationssicherheitsbeauftragten beim **rbb** nach wie vor nicht als Stabsstelle mit unmittelbarer Anbindung an die Geschäftsleitung eingerichtet worden ist, wodurch seine unabhängige Stellung unterstrichen worden wäre, sondern der Stabsabteilung OUI innerhalb der Verwaltungsdirektion zugeordnet ist.

Immerhin kann sich der Informationssicherheitsbeauftragte auf Tz. 4.1 Abs. 2 der Dienstanweisung zur Gewährleistung der Informationssicherheit vom 23. April 2014 stützen. Darin ist geregelt, dass er in seiner Funktion fachlich unabhängig ist.

B. Entwicklung des Datenschutzrechts

I. Europa

1. Normen

1.1 EU Datenschutz-Grundverordnung

Am 4. Mai 2016 wurde die Europäische Datenschutz-Grundverordnung (DS-GVO) im Amtsblatt der Europäischen Union veröffentlicht. 20 Tage später ist sie in Kraft getreten. Ab dem 25. Mai 2018 wird sie für Behörden und Unternehmen in ganz Europa unmittelbar gelten.

Die DS-GVO mit ihren 99 Artikeln und 173 Erwägungsgründen ist deutlich umfangreicher als das Bundesdatenschutzgesetz. An einigen Stellen enthält sie Öffnungsklauseln, die die nationalen Gesetzgeber verpflichten bzw. berechtigen, auf nationaler Ebene zusätzlich bestimmte Regelungsbereiche auszugestalten. Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sowie alle anderen bereichsspezifischen Regelungen, für die es keine ausdrückliche Öffnungsklausel gibt, werden aller Voraussicht nach durch die allgemeinen Normen der DS-GVO verdrängt.

Die Herausforderung besteht somit darin, sich mit dem Regelungswerk der DS-GVO vertraut zu machen, den individuellen Umstellungsbedarf festzustellen und dabei die laufende Gesetzgebung zum Datenschutz auf nationaler Ebene nicht unberücksichtigt zu lassen.

Die DS-GVO schreibt im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien fort und entwickelt sie weiter. Die aus der EU-Datenschutzrichtinie und den deutschen Datenschutzgesetzen bekannten Grundsätze des „Verbots mit Erlaubnisvorbehalt“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“ und der „Transparenz“ prägen auch die DS-GVO.

Die DS-GVO enthält jedoch auch einige neue Elemente. Zum einen ist in diesem Zusammenhang das sog. Marktortprinzip zu nennen, nach dessen Maßgabe das EU-Datenschutzrecht auch für Wirtschaftsunternehmen außerhalb der Europäischen Union gilt. Voraussetzung ist lediglich, dass sich ein Angebot an einen bestimmten nationalen Markt in der EU richtet oder dass die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient. Interessant wird in diesem Zusammenhang unter anderem die Entwicklung bei den sog. Sozialen Netzwerke wie z. B. bei Facebook, Twitter und youtube werden. Diese Anbieter erfüllen derzeit aus verschiedenen Gründen nicht die deutschen Datenschutzstandards. Bedenken bestehen insbesondere in Bezug auf die Anforderungen an Transparenz, Datensparsamkeit und wirksame Einwilligung. Die meisten Anbieter speichern die Daten zudem außerhalb der EU in Ländern wie den USA, die kein vergleichbares Niveau an Datenschutz gewährleisten. Es bleibt abzuwarten, ob diese Unternehmen vor dem Hintergrund der DS-GVO hier nachbessern.

Im Bereich des Minderjährigen-Datenschutzes trifft die DS-GVO eine klare Aussage: Für eine rechtswirksame Einwilligung in die Datenverarbeitung kommt es nicht auf die Geschäftsfähigkeit einer Person an. Jugendliche, die mindestens 16 Jahre alt sind, können über ihre personenbezogenen Daten eigenverantwortlich verfügen. Der nationale Gesetzgeber kann dieses Mindestalter sogar noch weiter herabsetzen, darf dabei ein Alter von 13 Jahren jedoch nicht unterschreiten.

Die DS-GVO strebt eine möglichst einheitliche Rechtsanwendung in der Europäischen Union an. Dies soll im Falle grenzüberschreitender Datenverarbeitungen im nicht-öffentlichen Bereich durch einen komplexen Kooperations- und Kohärenzmechanismus umgesetzt werden, an dessen Ende eine einheitliche Entscheidung der Aufsichtsbehörden der EU-Mitgliedstaaten zur Rechtsanwendung steht.

1.2 Europäische Richtlinie zur Sicherheit von Netz- und Informationssystemen

Am 19. Juli 2016 ist die Europäische Richtlinie zur Sicherheit von Netz- und Informationssystemen im Amtsblatt der Europäischen Union veröffentlicht worden. Neben den Aufgaben für die Staaten, für die Sicherheit von Netz- und Informationssystemen zu sorgen, findet sich darin auch die Verpflichtung, Sicherheitsanforderungen und Meldepflichten für die „Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste aufzustellen. Welche Dienste wesentlich i. S. dieser Richtlinie sind, ergibt sich aus einer Aufzählung im Anhang II der Richtlinie. Dort findet man als letzten Punkt zwar den Sektor „digitale Infrastruktur", nicht aber die Rundfunkanstalten. Das heißt, dass die Rundfunkanstalten von dieser Richtlinie nicht tangiert sind.

2. Urteile

2.1 Safe Harbor

Nach den Regelungen der EU-Datenschutzrichtlinie ist eine Übermittlung personenbezogener Daten ins EU-Ausland (sog. Drittländer) grundsätzlich nur zulässig, wenn und soweit dort ein mit den europäischen Datenschutzregelungen vergleichbares Datenschutzniveau gewährleistet wird. Am 6. Oktober 2015 hat der Gerichtshof der Europäischen Union (EuGH) das sog. Safe Habor-Abkommen zwischen der EU-Kommission und den USA für ungültig erklärt. Zuvor hatte die EU-Kommission Unternehmen in den USA, die sich den Safe Harbor-Regelungen unterworfen hatten, ein angemessenes Schutzniveau für personenbezogene Daten bescheinigt mit der Folge, dass die Datenübermittlung aus einem Land der Europäischen Union in die USA zulässig war. Den nationalen Datenschutzbehörden war es dadurch nicht mehr gestattet, die Zulässigkeit der Übermittlung personenbezogener Daten in die USA selbst zu prüfen.
Vor dem Hintergrund der Enthüllungen von Edward Snowden hat der EuGH die Selbsterklärung der Firmen nach dem Safe Harbor-Abkommen nicht mehr für ausreichend angesehen. Denn die Safe Harbor-Regelungen enthielten keine Beschränkungen der Eingriffsrechte der US-Behörden. Außerdem gab es für die Betroffenen keine wirksamen Rechtsschutzmöglichkeiten.

Im Februar 2016 ist eine neue Vereinbarung mit den USA, das Privacy-Shield vereinbart worden. Die US-Administration hat der EU-Kommission einen besseren Schutz für Daten aus der EU schriftlich zugesichert. Unter anderem sollen Überwachungsmaßnahmen auf das „Notwendige und Verhältnismäßige" begrenzt werden und jährliche Berichte von US-Seite an die Kommission ergehen.
Ungeachtet der Kritik der Europäischen Datenschutzbehörden und des Europäischen Parlaments an dem Privacy Shield, dass auch dieses Abkommen massenhaft Informationen im Dienste der öffentlichen Sicherheit zu sammeln ermögliche, haben die meisten EU-Staaten den neuen – nachgebesserten - Regeln für den Datenaustausch zugestimmt. Daraufhin hat die EU-Kommission das Privacy Shield am 12.Juli 2016 förmlich verabschiedet. Sie wird jährlich einen Bericht über die Erfahrungen mit dem Privacy Shield erstellen und diesen dem Europäischen Parlament und dem Europäischen Rat zuleiten. Die Überprüfung wird von der Kommission gemeinsam mit dem US-Handelsministerium durchgeführt.

Es bleibt abzuwarten, ob der EuGH sich demnächst auch mit der Wirksamkeit des Privacy Shield befasst wird.

Als Alternative zum Privacy Shield gibt es derzeit noch andere Mittel für eine rechtmäßige Datenübertragung in die USA – neben einer ausdrücklichen Einwilligung der Nutzer in den Datentransfer - die Standardvertragsklauseln der EU und sog. Binding Corporate Rules. Die Standardvertragsklauseln sind Vertragsklauseln, die beim Datenempfänger ein angemessenes Datenschutzniveau sicherstellen sollen. Ob die EU-Standardvertragsklauseln langfristig Bestand haben werden, ist derzeit nicht absehbar. Nach einhelliger Auffassung sind auch diese datenschutzrechtlich problematisch. Denn das vom EuGH in seiner „Safe Harbor"-Entscheidung aufgezeigte Kernproblem besteht in der Schutzlosigkeit amerikanischer Unternehmen vor staatlichen Übergriffen. Das Risiko eines Zugriffs amerikanischer Behörden auf personenbezogene Daten ist auch durch die Verwendung von EU-Standardvertragsklauseln nicht ganz ausgeräumt. Dennoch dürfte die Nutzung dieses Instruments bis zu einer anderslautenden Entscheidung des EuGH weiterhin vertretbar sein.

Die hier skizzierte Entwicklung hat auch für den **rbb** unmittelbar Relevanz, z. B. beim zukünftigen Einsatz von Cloud-basierten Lösungen. Das bislang im **rbb** noch bestehende generelle Verbot der Nutzung von online-Speichermöglichkeiten in der Cloud wird aufgrund betrieblicher Notwendigkeiten mittelfristig nicht aufrecht zu halten sein (s. C I 6.). Es gilt, differenzierte Lösungen zu finden. Was allerdings die Zusammenarbeit mit US-Anbietern betrifft, kommt zu der Schwierigkeit des unterschiedlichen Datenschutzniveaus noch folgendes hinzu:

In seinem Tätigkeitsbericht für das Jahr 2014 weist der Berliner Datenschutzbeauftragte darauf hin, dass das für den **rbb** maßgebliche Berliner Datenschutzgesetz (BlnDSG) überhaupt keine Datenweitergabe an Drittstaaten (Staaten außerhalb der EU) im Rahmen der Auftragsdatenverarbeitung vorsieht. Während eine Wartung außerhalb der Europäischen Union im Gesetz erwogen wird (§ 3a Abs. 1 Ziffer 10 BlnDSG), fehlt ein entsprechender Hinweis für die sonstige Auftragsdatenverarbeitung völlig. (Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2014, S. 32). Herr Dr. Dix hat aus diesem Umstand auch praktische Konsequenzen gezogen. So rät er beispielsweise von der Nutzung des Microsoft-Produkts Office 365 gänzlich ab (Dix, aa0, S. 33). Angesichts der Mängel beim Datenschutz in den USA hat er überdies Bildungssenatorin Sandra Scheeres aufgefordert, Lehrern die dienstliche Kommunikation mit Schülern über soziale Medien wie Facebook oder Whatsapp zu untersagen (Tagesspiegel vom 16.10.2015, S. 10).

II. Bund

1. Normen

1.1 Informationssicherheitsgesetz

Am 25. Juli 2015 ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (Informationssicherheitsgesetz) in Kraft getreten. Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen müssen künftig einen Mindeststandard an Informationssicherheit einhalten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt

für Sicherheit in der Informationstechnik (BSI) melden. Darüber hinaus sind zur Steigerung der Informationssicherheit im Internet die Anforderungen an die Anbieter von Telekommunikations- und Telemediendiensten erhöht worden. Parallel dazu sind die Kompetenzen des BSI und der Bundesnetzagentur sowie die Ermittlungszuständigkeiten des Bundeskriminalamtes (BKA) im Bereich der Computerdelikte ausgebaut worden.

Den Kritikern geht das Gesetz nicht weit genug. Es wird moniert, dass es in dem Gesetz zu viele unbestimmte Rechtsbegriffe gibt. Die vorgesehenen Maßnahmen seien nicht geeignet, zur Erhöhung der Informationssicherheit in Deutschland beizutragen. Vor dem Hintergrund der sensiblen Informationen, die das BSI durch die Meldungen von Sicherheitsvorfällen erhalte, wird zudem eine unabhängige Stellung des BSI, das derzeit dem Bundesinnenministerium unterstellt und verpflichtet ist, gefordert.

Die Landesrundfunkanstalten sind aus kompetenzrechtlichen Gründen nicht Adressaten dieses Bundesgesetzes.

Dass zumindest Teile der Medien durchaus als kritische Infrastrukturen verstanden werden, dürfte jedoch nach dem groß angelegten Angriff auf die französische Fernsehsendergruppe TV5Monde Anfang April 2015 inzwischen einhellige Meinung sein.
Insoweit empfiehlt es sich, dass sich der **rbb** an dem im Informationssicherheitsgesetz vorgeschriebenen Mindeststandard an Informationssicherheit zumindest orientiert. Auch vor diesem Hintergrund halte ich es für notwendig, den Themen Datenschutz und Informationssicherheit im **rbb** noch mehr Gewicht als bislang einzuräumen. Zukünftig sollten Informationssicherheitsanforderungen in alle Verträge für IT-Systeme und Leistungen mit den Anbietern aufgenommen werden. Im Übrigen werden wir die legislativen Entwicklungen auf diesem Gebiet weiterhin sehr aufmerksam verfolgen.

1.2 Telemediengesetz

Am 27. Juli 2016 ist das geänderte Telemediengesetz (TMG) in Kraft getreten. Mit der Gesetzesänderung soll klargestellt werden, dass Betreiber von öffentlichen Funknetzen (WLAN) ebenso von der Haftung für Rechtsverstöße Dritter freigestellt sind wie Festnetzanbieter.

Von dieser Gesetzesänderung ist der **rbb** unmittelbar betroffen. Denn auch er bietet seinen Gästen regelmäßig WLAN an.

Der Gesetzesänderung ging ein jahrelanges Tauziehen voraus, an dessen Ende ein Kompromiss steht, der von Experten kritisiert wird. Erst die Praxis wird zeigen, ob die Gesetzesänderung tatsächlich auch vor zivilrechtlicher Inanspruchnahme des WLAN-Betreibers schützt.

Möglicherweise wird es im Laufe des Jahres noch eine neue Entwicklung geben. Denn in einem beim EuGH anhängigen Verfahren, das das Münchner Landgericht vorgelegt hatte, wird dieser Ansprüche von Sony Music gegen eine Person, die ein offenes WLAN betreibt, prüfen.

Bis zur endgültigen Klärung sollte der **rbb** dabei bleiben, zur Vermeidung einer Inanspruchnahme im Rahmen der sog. Störerhaftung angemessene Sicherungsmaßnahmen zu ergreifen und Zugang zum Internet nur denjenigen Nutzern zu gewähren, die erklärt haben, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen.

1.3 Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts

Am 24. Februar 2016 ist das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts in Kraft getreten. Durch dieses Gesetz werden unter anderem die Abmahnbefugnisse von Verbraucherschutzverbänden auf datenschutzrechtliche Verstöße erweitert.

Wie schon in meinem letzten Tätigkeitsbericht erwähnt, sehen die Datenschutzbeauftragten diese Entwicklung nicht unkritisch. Der Datenschutz wird danach stärker als bislang dem Einfluss von Entscheidungen der Zivilgerichte ausgesetzt. Hieraus ist eine gewisse Konkurrenz zur Tätigkeit der datenschutzrechtlichen Aufsichtsbehörden, denen das Gesetz allerdings ein Anhörungsrecht einräumt, zu erwarten. Es besteht die Sorge, dass die Zivilgerichte bei ihrer einzelfallbezogenen und durch den Klageanspruch limitierten Tätigkeit nicht unbedingt die datenschutzrechtlichen Gegebenheiten in umfassender und korrekter Weise abbilden können.

1.4 Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherdauer für Verkehrsdaten

Am 18. Dezember 2015 ist das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten in Kraft getreten. Danach müssen Telekommunikationsunternehmen Internet- und Verkehrsdaten jedes Bürgers anlasslos für zehn Wochen speichern. Das umfasst solche technischen Informationen, die bei der Nutzung eines Telekommunikationsdienstes (Telefonie, Internetnutzung) beim jeweiligen Telekommunikationsunternehmen (Provider) anfallen. Daneben sind Standortdaten vier Wochen zu speichern. Die entsprechenden Inhalte dürfen dagegen nicht dokumentiert werden.

Dies ist ein weiterer Versuch, ein Gesetz zu schaffen, das die anlasslose Speicherung von Daten einer Vielzahl von Menschen für öffentliche Stellen zum Gegenstand hat. Am 2. März 2010 hatte das Bundesverfassungsgericht (BVerfG) ein Vorgängergesetz gestoppt und für verfassungswidrig erklärt. Zwar verstoße eine Vorratsdatenspeicherung nicht generell gegen das Grundgesetz, jedoch seien die Rahmenbedingungen in dem Gesetz nicht hinreichend festgelegt. Das damalige Gesetz basierte auf einer entsprechenden EU-Richtlinie, die - ich hatte in meinen früheren Tätigkeitsberichten berichtet - der EuGH mit Urteil vom 8. April 2014 für ungültig erklärt hat. Nach Auffassung der erkennenden Richterinnen und Richter beinhaltete die Regelung einen „Eingriff von großem Ausmaß und besonderer Schwere in die

Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, der sich nicht auf das absolut Notwendige beschränkt."

In einer gemeinsamen Stellungnahme hatten ARD und ZDF, der Bundesverband Deutscher Zeitungsverleger, der Deutsche Journalisten Verband, der Deutsche Presserat, der Verband Deutscher Zeitschriftenverleger, die Vereinte Dienstleistungsgewerkschaft und der Verband Privater Rundfunk und Telemedien im Vorfeld das Gesetzesvorhaben kritisiert, weil es die Pressefreiheit gefährde. Die Speicherung von Telefonnummern, IP-Adressen und Standortdaten untergrabe den Schutz der Informanten, zu dem insbesondere Journalistinnen und Journalisten berechtigt und ethisch verpflichtet sind. Zudem fehle es an einem Schutz von Berufsgeheimnisträgern vor der Speicherung ihrer elektronischen beruflichen Kontakte. Genau das Fehlen eben solcher Regelungen hatte der EuGH in seiner oben genannten Entscheidung vom 8. April 2014 an der nunmehr für ungültig erklärten EU-Richtlinie beanstandet.

Ob das neue Gesetz die verfolgte Zielsetzung der effektiven Bekämpfung der Kriminalität und des Terrorismus tatsächlich fördert, ist nach wie vor fraglich. Statistiken belegen dies bis heute nicht.

Nachdem die Gegner des Gesetzes unmittelbar nach seinem Inkrafttreten rechtliche Schritte angekündigt hatten, haben einige Bundestagsabgeordnete sowie Journalisten- und Medienverbände beim Bundesverfassungsgericht eine einstweilige Anordnung beantragt, weil sie sich als betroffene Berufsgeheimnisträger sehen. Sie wollten erreichen, dass die Speicherpflicht der Telekommunikationsanbieter bis zur Entscheidung über eine Verfassungsbeschwerde ausgesetzt wird. Der Antrag auf Erlass einer einstweiligen Anordnung wurde am 12. Januar 2016 abgelehnt, die Verfassungsbeschwerde ist weiterhin anhängig.

2. Urteile

2.1 Urteil des Bundesverfassungsgerichts zum BKA-Gesetz

Mit Urteil vom 20. April 2016 hat das BVerfG entschieden, dass die Ermächtigung des BKA zum Einsatz von heimlichen Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus zwar im Grundsatz mit den Grundrechten vereinbar ist, die derzeitige Ausgestaltung von Befugnissen aber in verschiedener Hinsicht dem Verhältnismäßigkeitsgrundsatz nicht genügt. Das führt dazu, dass verschiedene Regelungen aus dem Gesamtkomplex zu beanstanden waren. Die Entscheidung betrifft, eine lange Rechtsprechung zusammenführend, sowohl die Voraussetzungen für die Durchführung solcher Maßnahmen als auch die Frage der Übermittlung der Daten zu anderen Zwecken an dritte Behörden sowie schließlich erstmals auch die Anforderungen an eine Weiterleitung von Daten an ausländische Behörden.

2.2 Vorlagebeschluss des Bundesverwaltungsgerichts zur Verantwortlichkeit für die beim Aufruf einer Facebook-Fanpage erhobenen Nutzerdaten

Das Bundesverwaltungsgericht hat mit Beschluss vom 25. Februar 2016 in einem Verfahren den EuGH angerufen, in dem es um die Beanstandung des Betriebs einer Facebook-Fanpage seitens einer privatrechtlich organisierten Wirtschaftsakademie Schleswig-Holstein durch die Datenschutzaufsichtsbehörde geht. Geklärt werden soll unter anderem, ob die Anbieter von Angeboten über Drittplattformen eine Verantwortlichkeit gegenüber ihren Nutzern trifft, die sie zu einer sorgfältigen Auswahl der Drittplattformen verpflichtet.

Diese Fragestellung betrifft auch den **rbb** unmittelbar, da auch er auf Drittplattformen vertreten ist. Neben der Präsenz auf den „Standardplattformen“ wie Facebook, Twitter und Google+ rücken zunehmend auch Kanäle der Kategorie „Direkte Kommunikation/Echtzeit“ wie WhatsApp (Text), Snapchat (Fotos, Video) und Periscope (Video) und „Fotos/Style“ wie z. B. Instagram in das Blickfeld des **rbb.**

Das Problem dabei ist, dass die meisten Anbieter von Drittplattformen ihren Sitz in den USA haben. Auch wenn sich die veröffentlichten Informationen und Nutzungsbedingungen der Anbieter fortlaufend ändern, muss bis auf weiteres davon ausgegangen werden, dass die Angebote nicht den deutschen Datenschutzstandards entsprechen. Namentlich wird den im Telemediengesetz zugrundeliegenden Prinzipien der Transparenz und Datensparsamkeit nicht hinreichend Rechnung getragen.

Bei Nutzung der Drittplattformen findet ein umfangreiches Tracking des Nutzerverhaltens für Zwecke der Werbung statt. Die Daten werden in der Regel auf Servern in den USA gespeichert. Dort werden den Ermittlungsbehörden etwa auf Grundlage des sog. *patriot acts* weitreichende Zugriffsbefugnisse eingeräumt.

Den Anbietern kommt dabei eine noch bestehende Rechtsunsicherheit zugute. Denn bislang ist nicht abschließend gerichtlich geklärt, ob die europäischen und nationalen Regelungen auch für außereuropäische Anbieter verbindlich sind, die ihr Angebot an einen bestimmten nationalen Markt in der EU richten. Erst die DS-GVO, die bis 2018 umgesetzt werden muss, schafft hier Klarheit. Nach dem sog. Marktortprinzip erstreckt sich der Anwendungsbereich zukünftig auch auf außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind. Es bleibt abzuwarten, welche Schlussfolgerungen die außereuropäischen Anbieter daraus innerhalb der nächsten Jahre ziehen werden.

In jedem Fall ist und bleibt die Präsenz der durch öffentliche Beiträge finanzierten Rundfunkanstalten auf den Drittanbieterplattformen auch aufgrund ihrer Vorbildfunktion problematisch. Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten empfehlen folgende Herangehensweise:

Es sollte im jeweiligen Einzelfall gewissenhaft abgewogen werden, ob der publizistische Mehrwert trotz der Mängel im Datenschutz für die Präsenz der Rundfunkanstalt auf dieser Plattform spricht. Es sollte geprüft werden, ob der jeweilige Anbieter im Rahmen einer eigenen Vereinbarung zur Einhaltung der deutschen Standards bewegt werden kann. Die Rundfunkanstalt sollte auf die Datenschutzmängel der Plattform hinweisen und ihre Präsenz auf Drittplattformen so datenschutzge-

recht wie möglich ausgestalten. Dies bedeutet z. B., dass die Rundfunkanstalten die Nutzer nicht dazu einladen dürfen, sensible Informationen über die Fanpage eines sozialen Netzwerks preiszugeben.

III. Berlin/Brandenburg

1. Rundfunkänderungsstaatsvertrag

Mit Gesetz vom 2. Juni 2016 (Berlin) bzw. vom 19. Mai 2016 (Brandenburg) haben Berlin und Brandenburg dem 19. Rundfunkänderungsstaatsvertrag zugestimmt. Der Staatsvertrag tritt mit Ausnahme der Änderungen zum Rundfunkbeitragsstaatsvertrag (Art. 4), die erst zum 1. Januar 2017 in Kraft treten, zum 1. Oktober 2016 in Kraft.

Aus datenschutzrechtlicher Sicht sind folgende Änderungen interessant:

Gemäß Artikel 1 Ziffer 5 wird ein neuer § 11 g in den Rundfunkstaatsvertrag als Rechtsgrundlage für das neue Jugendangebot von ARD und ZDF eingefügt. Gemäß § 11 g Abs. 5 Satz 3 haben ARD und ZDF für die Verbreitung außerhalb des für das Jugendangebot eingerichteten eigenen Portals auf Drittplattformen übereinstimmende Richtlinien, insbesondere zur Konkretisierung des Jugendmedienschutzes und des *Datenschutzes* zu erlassen. Mit der Erstellung des Entwurfs der Datenschutz-Richtlinien sind die Datenschutzbeauftragten von ARD und ZDF derzeit befasst.

Gemäß Artikel 4 Ziffer 7 werden die konkretisierenden datenschutzrechtlichen Regelungen, die sich bislang in den Rundfunkbeitragssatzungen befanden, in den Rundfunkbeitragsstaatsvertrag übernommen.

Die Befugnis zum Adressankauf wird bis zum 31. Dezember 2020 weiter ausgesetzt. Stattdessen ist ein weiterer vollständiger Meldedatenabgleich im Rundfunkbeitragsstaatsvertrag vorgesehen.

Die Rundfunkdatenschutzbeauftragten von ARD, ZDF und DLR hatten sich – wie im letzten Tätigkeitsbericht erwähnt - in ihrer Stellungnahme zum Entwurf des 19. Rundfunkänderungsstaatsvertrags für die entsprechenden Änderungen ausgesprochen. Aus ihrer Sicht haben die Rundfunkanstalten überzeugend dargelegt, dass allein die staatsvertraglichen Anzeigepflichten und Auskunftsrechte nicht ausreichen, um einer erneuten Erosion des Teilnehmerbestandes wirksam vorzubeugen. Die Durchführung eines erneuten Meldedatenabgleichs ist nach unserer Überzeugung das mildeste und am besten geeignete Mittel, diesen Entwicklungen vorzubeugen – dies vor dem Hintergrund der strikten Zweckbindung und der in Praxis problemlosen und von wenig Beschwerden begleiteten reibungslosen Durchführung des Meldedatenabgleichs im Jahre 2013.

C. Datenschutz und Datensicherheit im rbb

I. Allgemeines

1. Dienstanweisung Auftragsdatenverarbeitung

Seit 2012 habe ich zusammen mit der OUI an einem Entwurf für die Dienstanweisung Auftragsdatenerarbeitung gearbeitet. Es fanden intensive Abstimmungsprozesse mit den Hauptadressaten der Dienstanweisung, den Mitarbeitern in der Abteilung Einkauf und den Projektleitern in der Produktions- und Betriebsdirektion, statt. Im Mai 2016 ist die Dienstanweisung endlich in Kraft getreten (Anlage). Die Dienstanweisung regelt das Verfahren bei der Vergabe und der Durchführung von Datenverarbeitung durch externe Firmen im Auftrag des **rbb** und von Wartungsarbeiten. Sie ersetzt die bisherigen Wartungsrichtlinien.

Auftragsdatenverarbeitung gibt es im **rbb** in unterschiedlichen Fällen wie z. B. beim Hosting von Internet-Angeboten, der Durchführung von Meinungsumfragen, der Beauftragung von Externen mit der Aufklärung von Rundfunkbeitragssachverhalten, der Verarbeitung von Versorgungsdaten etc. Neben den allgemeinen Regeln zur Durchführung der Auftragsdatenverarbeitung sind in der Dienstanweisung auch

Maßnahmen zur Nutzung des **rbb**-Kommunikationsnetzes, Maßnahmen bei Fernzugriffsverfahren und Maßnahmen bei Transport von IT-Systemen und deren Komponenten aufgeführt.
Mit diesem neuen Regelwerk wird sichergestellt, dass der **rbb** seiner Verantwortung zum Schutz personenbezogener Daten und der Betriebs- und Geschäftsgeheimnisse gerecht wird und entsprechende vertragliche Regelungen mit den Auftragnehmern trifft sowie die Arbeiten der Auftragnehmer angemessen überwacht.

Verantwortlich für die Umsetzung der in der Dienstanweisung beschriebenen Maßnahmen ist die jeweils fachlich verantwortliche Organisationseinheit.

2. Dienstanweisung IT-Nutzung

Anfang März 2016 hat mir die OUI den Entwurf einer Dienstanweisung für die Nutzung von IT zur Prüfung vorgelegt.

In der Dienstanweisung IT-Nutzung sollen die Regelungen zur Nutzung von Hard- und Software, die sich bislang in unterschiedlichen Dienstanweisungen finden, zusammengefasst, ergänzt und aktualisiert werden. Ein weiterer Regelungsgegenstand soll die Nutzung von Datendiensten (Internet und E-Mail, zentrale Datenspeicherung) sein. Die bisherige Dienstanweisung zur Nutzung von Internet und E-Mail soll darin aufgehen.

Wie schon in meinem letzten Tätigkeitsbericht erwähnt, ist im **rbb** die Nutzung von Hard- und Software bislang nur teilweise geregelt, so dass ich es grundsätzlich begrüße, dass in der neuen Dienstanweisung für diese Themen zukünftig klare Regelungen geschaffen werden. Ideal wäre es aus meiner Sicht gewesen, zunächst für sämtliche beabsichtigten Regelungsbereiche klare inhaltliche Vorstellungen und Konzepte zu entwickeln und erst im Anschluss daran die Dienstanweisung zu formulieren. So muss im Hinblick auf die Nutzung von mobilen Geräten wie Smartphone, Laptop etc. das Konzept für die Datensicherheit noch überarbeitet werden (s.6.). Auch die Frage nach einer möglichen Nutzung von privaten Geräten für

dienstliche Zwecke und ggf. die Modalitäten der Nutzung müssen geklärt werden (s. Nr.7). Außerdem fehlt im **rbb** bislang eine Cloud-Strategie (s. 8.).

Die Kolleginnen und Kollegen aus der OUI haben mich allerdings davon überzeugt, dass der Handlungsdruck zum Erlass der Dienstanweisung inzwischen so groß ist, dass es nicht möglich ist, sämtliche abschließenden Klärungen abzuwarten, sondern zur Not mit einer unvollständigen Dienstanweisung zu starten, die dann im Laufe der Zeit noch komplettiert wird.

Die Abstimmungen mit der OUI über Detailfragen zum geplanten Inhalt dauern noch an.

3. Informationssicherheitskreis

Wie in den vergangenen beiden Tätigkeitsberichten erwähnt, existiert seit 2014 die Dienstanweisung zur Gewährleistung der Informationssicherheit. Darin ist unter anderem die Organisationsstruktur des Informationssicherheits-Managements des **rbb** geregelt. Die Aufgaben des Informationssicherheitsbeauftragten werden im Einzelnen aufgelistet. Der Informationssicherheitsbeauftragte wird durch den Informationssicherheitskreis (ISK) unterstützt, dem auch die Datenschutzbeauftragte angehört. Der ISK hat bislang erst ein einziges Mal, am 1. Juni 2015, getagt. Das Ziel, dass der ISK sich künftig vier Mal im Jahr trifft, um Fragen zur Informationssicherheit zu erörtern, konnte bislang nicht umgesetzt werden. Geschuldet war dies wohl vor allem der Doppelbelastung des bisherigen Informationssicherheitsbeauftragten, der ja auch und vor allem Bereichsleiter des IT-Betriebes beim **rbb** ist. Es bleibt zu hoffen, dass der neue Informationssicherheitsbeauftragte, der seit dem 1. Juli 2016 im Amt ist, auch den ISK neu belebt.

4. Regeltermin IT-Projekte

In regelmäßigen Terminen informiert OUI die Mitglieder des Personalrates, 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 möglichst frühen Zeitpunkt zu reklamieren. Im Berichtszeitraum fanden Termine am 9. April, 16. Juli und 7. Dezember 2015 und am 13. Juni 2016 statt.

5. Technisches Sicherheitskonzept für die Liegenschaften des rbb

In meinem letzten Tätigkeitsbericht habe ich darüber berichtet, dass ein technisches Sicherheitskonzept für die Liegenschaften des **rbb** in Planung sei. Dieses Sicherheitskonzept liegt laut der zuständigen Abteilungsleiterin jetzt vor und soll demnächst der Geschäftsleitung vorgestellt werden.

Ich gehe davon aus, dass das Konzept auch dem Informationssicherheitsbeauftragten und mir nun zeitnah zur Prüfung vorgelegt wird. Aus meiner Sicht ist es insbesondere vor dem Hintergrund der andauernden Gefährdungslage unverzichtbar, möglichst bald zu konkreten Lösungen zu kommen, die sämtliche Eingänge, die speziell zu schützenden Räume wie z. B. die Serverräume und auch das Parkhaus mit einbeziehen.

6. Erstellung eines Informationssicherheitskonzepts für mobile Endgeräte

Zur Erhöhung der Datensicherheit der **rbb**-eigenen mobilen Endgeräte müssen zusätzliche technische und organisatorische Maßnahmen ergriffen werden. Zu diesem vorläufigen Ergebnis kommt eine externe Beratungsfirma, die – auf mein Drängen - im Sommer 2015 mit der Erstellung eines Informationssicherheitskonzeptes für mobile Endgeräte sowie der Erstellung einer Richtlinie zur Nutzung der Geräte im Rahmen des **rbb**-Sicherheitskonzepts beauftragt worden ist.

Im Berichtszeitraum haben mehrere Gespräche mit dem Auftragnehmer stattgefunden, an denen ich jeweils teilnahm. Dabei ging es bislang um die Konkretisierung des Auftrags und um die Besprechung von Zwischenergebnissen. Die abschließenden Ergebnisse werden derzeit vom Informationssicherheitsbeauftragten geprüft.

7. Bring your own device

Zunehmend löst sich die Grenze zwischen beruflicher und privater IT-Nutzung auf. Viele Systeme, Programme und Dienste werden mittlerweile sowohl im beruflichen wie auch im privaten Umfeld genutzt.

Vor allem im journalistischen Bereich gibt es inzwischen den Wunsch vieler Mitarbeiterinnen und Mitarbeiter, für ihre dienstliche Tätigkeit im **rbb** ihre privaten mobilen IT-Geräte wie Tablets, Smartphones und Laptops zu nutzen. Das hat für die Nutzer unter anderem den Vorteil, dass sie nicht parallel mit zwei mobilen Geräten gleichzeitig umgehen müssen – mit einem für dienstliche und einem anderen für private Zwecke. Relevant wurde dieses Thema im **rbb** bislang bei der Nutzung der MuPro-App (s. II 6.) und der ARD-Box (s. II 7.). Auch weitere Anwendungen wie der Zugriff auf die dienstlichen Mail und den dienstlichen Kalender von privaten Geräten aus werden von einigen Kolleginnen und Kollegen gewünscht.

Vereinzelt wurde dem Wunsch der Kolleginnen und Kollegen – ausschließlich für IOS-Geräte - bereits nachgegeben, ohne dass es bislang ein schlüssiges Gesamtkonzept für den Einsatz privater Geräte (=„Bring your own device", BYOD) im **rbb** gibt. Die Erarbeitung eines solchen Konzeptes ist aber unerlässlich, denn BYOD birgt eine Menge Risiken, insbesondere, wenn ein Privatgerät mit der **rbb**-IT verbunden wird.

Der **rbb** bleibt als im datenschutzrechtlichen Sinne verantwortliche Stelle auch dann für die ordnungsgemäße Verarbeitung von personenbezogenen Daten haftungsrechtlich verantwortlich, wenn die Datenverarbeitung auf privaten Geräten der Beschäftigten stattfindet. Aber anders als bei Geräten, die Eigentum des **rbb** sind, hat der **rbb** ohne vorhergehende Vereinbarungen nur sehr eingeschränkte Möglichkeiten, technische und organisatorische Vorgaben hinsichtlich der sicheren Datenverarbeitung auf Privatgeräten zu treffen und diese auch durchzusetzen.

Daher liegt die Forderung nahe, auf BYOD ganz zu verzichten. Andererseits habe ich Verständnis dafür, dass gerade der **rbb** als modernes Medienunternehmen sich

nicht dem allgemeinen Trend widersetzten kann. Es kommt daher aus meiner Sicht entscheidend darauf an, eine klare Vereinbarung mit den Mitarbeiterinnen und Mitarbeitern zu schließen, in der mindestens die folgenden Themen geregelt sind:

- Freiwilligkeit des Einsatzes von Privatgeräten,
- Vorgabe zur Trennung privater und geschäftlicher Daten,
- Regelung zum Zugriff des **rbb** auf Daten,
- Regelung zur Frage, in welchen Fällen der **rbb** Daten löschen darf,
- Regelung zum Einsatz von Monitoringtools,
- Vorgaben zur festen Einstellung von Systemparametern,
- Regelung zur Haftungsverteilung,
- Mitteilungspflicht bei Verlust,
- Nutzung des privaten Gerätes durch Dritte und
- Durchführung von Reparatur- und Wartungsarbeiten.

8. Leitlinien für die Nutzung von Cloud-Technologien

Cloud Computing kann unter anderem dazu genutzt werden, über ein Netz dynamisch an den Bedarf angepasst IT-Dienstleistungen, insbesondere Speicherkapazitäten, zu nutzen. Die Nutzung der Cloud eines externen Anbieters für Online-Speichermöglichkeiten ist beim **rbb** bislang generell verboten. Allerdings nimmt die Bedeutung von Cloud-Lösungen stetig zu. Ihre Nutzung bietet Chancen und Vorteile. Die Vorteile liegen darin, dass Speicherkapazitäten und Rechenleistungen je nach Bedarf flexibel und dadurch sehr wirtschaftlich eingesetzt werden können. Die Nutzung birgt aber auch Probleme und Risiken:

Wenn Unternehmensdaten „in der Cloud“ gespeichert und verarbeitet werden, wirft das Fragen in Bezug auf die Datensicherheit und den Schutz vertraulicher Informationen auf. Die Nutzung von Cloud-Technologien erfolgt im Rahmen der Auftragsdatenverarbeitung. Das heißt, dass der **rbb** für die Sicherheit der extern gespeicherten Daten verantwortlich bleibt. Der Cloud-Dienstleister muss wiederum mindestens dasselbe Datenschutzniveau bieten wie der **rbb.**

Das generelle Problem besteht darin: Viele Cloud-Anbieter sind amerikanische Firmen, die laut Gesetz verpflichtet sind, US-Behörden Zugriff auf alle Daten in der Cloud zu geben, auch wenn sich die Rechnerparks auf europäischem oder deutschen Boden befinden. Aus deutscher Datenschutzsicht ist das nicht akzeptabel.

Wie schon in meinem letztjährigen Tätigkeitsbericht mitgeteilt, bietet das Informations- und Verarbeitungszentrum (IVZ) den ARD-Anstalten eine interne Cloud-Lösung für Online-Speicher an (s. D). Das Hosting der Applikation und der Daten erfolgt datenschutzkonform auf der IT-Infrastruktur des IVZ. Der Zugriff auf die Dateien erfolgt per Web-Browser und mittels App per mobilem Endgerät von registrierten Nutzern der Rundfunkanstalten.

Die ARD-Box bietet eine gute Möglichkeit der externen Speicherung von überschaubaren Datenmengen. Insofern kann es bei dem strikten Verbot der Nutzung einer public cloud für die normalen user im **rbb** bleiben. Die Nutzung der ARD-Box ist allerdings vor allem für den Datenaustausch vorgesehen und empfiehlt sich hingegen nicht für zeitkritische Zugriffe auf (hochauflösende) Videodateien, da es längere Lade – und Speicherzeiten geben kann. Für diesen Zweck steigt aber im **rbb** der Bedarf einer zentralen Lösung.

Im März 2016 hat mir der Verwaltungsdirektor vermittelt, dass er es daher begrüßen würde, wenn ich gemeinsam mit der OUI eine Leitlinie für die Nutzung von Cloud-Diensten im **rbb** erarbeiten würde. Ein erstes Treffen mit den Kollegen der OUI und anderen betroffenen Mitarbeitern des Hauses dazu hat am 24. Mai 2016 stattgefunden. Dabei wurde deutlich, dass zunächst einmal der Bedarf an Einsätzen der Cloud-Technologien im **rbb** konkret ermittelt werden muss, um daraus eine Cloud-Strategie bzw. Leitlinien für die Nutzung von Cloud-Diensten für den **rbb** ableiten zu können. Diese Aufgabe werden wir gemeinsam mit unserem neuen Informationssicherheitsbeauftragten jetzt angehen.

9. SAP-Dienstvereinbarungen

9.1 Aktualisierung der SAP-Dienstvereinbarungen

Wie in meinen früheren Tätigkeitsberichten erwähnt, müssen sämtliche beim **rbb** vorhandenen SAP-Dienstvereinbarungen wegen eines schon im Jahre 2009 stattgefundenen SAP-Releasewechsels von R/3 zu ERP 6.0 angepasst werden. Die Aktualisierungen der Dienstvereinbarungen waren über Jahre aus Kapazitätsgründen nicht erfolgt. Der Personalrat hat den Releasewechsel genutzt, um insbesondere Verhandlungen über Fragen zur Gewährleistung des Datenschutzes, des Arbeits- und Gesundheitsschutzes, der Systemschulungen sowie zur Klärung von Rechtsgrundlagen und Aufbewahrungsfristen von Reports einzufordern.

Nachdem im Jahr 2014 die Dienstvereinbarung zu dem Modul für Personaldatenverarbeitung HCM abgeschlossen werden konnte, folgten im April 2016 Abschlüsse der Dienstvereinbarungen SAP-KMH und FI im Rahmen einer Einigungsstelle. In die Verhandlungen mit dem Personalrat wurde ich einbezogen.

9.2 Umsetzung der SAP-Dienstvereinbarungen

Auch im Berichtszeitraum konnten die notwendigen Löschungen auf der Grundlage der in den Dienstvereinbarungen festgelegten Löschfristen für personenbezogene Daten noch nicht realisiert werden. In dieser Angelegenheit fanden mehrere Gespräche mit den verantwortlichen Mitarbeitern der Personalabteilung, der OUI und des IVZ statt.

Inzwischen waren zwei Kollegen aus der OUI bzw. dem IVZ bei SAP in Walldorf und haben neue technische Möglichkeiten in Erfahrung gebracht. Nun dürfte den Löschungen eigentlich nichts mehr im Wege stehen. Ich bleibe am Ball.

II. Aktuelle IT-Projekte

1. Openmedia/Multimediales Redaktions- und Planungssystem (MRPS)

Wie in meinen früheren Tätigkeitsberichten erwähnt, stellt der **rbb** seine Redaktionen derzeit multimedial auf. Das multimediale Redaktions- und Planungssystem OpenMedia ist das zentrale Werkzeug für die übergreifende Zusammenarbeit zwischen Fernsehen, Hörfunk und Online. Die redaktionellen Mitarbeiter recherchieren in diesem System ihre Themen und planen ihre Beiträge und Sendungen.

Leider konnte meine Vorabkontrolle, die neben der Zustimmung des Personalrats bzw. einer entsprechenden Dienstvereinbarung Voraussetzung für den Regelbetrieb ist, immer noch nicht abgeschlossen werden, weil die dazu erforderlichen Dokumente noch unvollständig sind. Dies betrifft die Auflistung aller personenbezogenen Mitarbeiterdaten, die im System verarbeitet werden, mit Angabe des Verwendungszwecks und der Rechtsgrundlagen, der Aufbewahrungsdauer, der Angabe, wer auf die Daten zugreifen darf und welche Schnittstellen es gibt sowie Angaben zu den Löschfristen. Den Gesprächen, die ich im Berichtszeitraum mit der Projektleitung geführt habe, habe ich entnommen, dass in der Vergangenheit insgesamt sehr weitgehende Berechtigungen eingeräumt worden sind und beim Anlegen der Berechtigungen nicht durchgängig geprüft wurde, ob die Kenntnis bestimmter Daten tatsächlich für den großen Kreis an zugriffsberechtigten Personen erforderlich ist. Dies ist – sofern es sich um journalistische Daten handelt – aufgrund des Medienprivilegs völlig problemlos. Gemäß § 36 Abs. 2 **rbb**-Staatsvertrag gelten neben den Bestimmungen des **rbb**-Staatsvertrages für solche Daten nur einige wenige Vorschriften des Bundesdatenschutzgesetzes entsprechend. Im Wesentlichen handelt es sich dabei um Vorschriften zur Datensicherheit. Für die Mitarbeiterdaten bedarf es jedoch einer genaueren Betrachtung. Erklärungsbedürftig wäre also etwa, warum ein Techniker auf dem Ü-Wagen wissen muss, welcher Reporter auf einer bestimmten Pressekonferenz war. Der Arbeitnehmerdatenschutz ist auch bei der internen Datenverarbeitung zu beachten. Mitarbeiterdaten dürfen nur verarbeitet werden wenn betriebliche Notwendigkeiten dies erfordern.

Es liegt nun die mühsame Aufgabe vor allen Beteiligten, die Dokumentation zu vervollständigen und ggf. nachträgliche Überarbeitungen vorzunehmen. Die Projektleitung hat dem Personalrat und mir zugesagt, diese Aufgabe nun zügig anzugehen.

2. Filebasierte Fernsehproduktion

Der **rbb** stellt seine technischen Systeme derzeit schrittweise auf eine durchgängig vernetzte filebasierte Fernsehproduktion im HDTV-Format um. Die filebasierte Fernsehproduktion basiert auf dem Zusammenwirken verschiedener technischer Komponenten. Diese sind im Einzelnen: der zentrale Ingest für das Einspielen des Bild- und Tonmaterials, Umwandlungssysteme für die Transcodierung in das HDTV-Haus-Format, Vorschau- und Steuerungssysteme für das zentrale Sichten und Verwalten aller Mediendateien, zentrale Speichersysteme, ein Content Management System - CMS, HDTV-Schnittplätze sowie ein multimediales Datennetzwerk für den schnellen Materialaustausch. Erst mit der vollständigen Einführung der filebasierten Fernsehproduktion im **rbb** erfolgt die vollständige Ablösung des Bandes. Die einzelnen Prozesse und Arbeitsabläufe, die Materiallogistik und -verwaltung geschieht für die Übergangszeit teilweise weiterhin „von Hand".
Dieser Umstellungsprozess ist wesentlicher Bestandteil des Unternehmensprojektes „Medienübergreifendes Arbeiten im Programm" (MAP) und wird pro Standort in mehreren Ausbaustufen realisiert. Im 1. Schritt wurde die filebasierte Fernsehproduktion für die Redaktionen Brandenburg Aktuell, zibb und WAS! in Potsdam eingeführt; im 2. Schritt erweitert der **rbb** die Einführung auf die Redaktion Abendschau in Berlin und in einem dritten Schritt für weitere Redaktionen an beiden Standorten.

Bei der filebasierten Fernsehproduktion werden nur wenige, allerdings notwendige personenbezogenen Daten der Nutzer verarbeitet. Die Inhaltsdaten unterfallen dem Medienprivileg. Für den Abschluss meiner Vorabkontrolle ist ein Informationssicherheitskonzept erforderlich, das derzeit erstellt wird.

3. Sendeabwicklung SAW

Der **rbb** hat sich entschlossen, die Sendeabwicklungstechnik Fernsehen am Standort Potsdam zu erneuern und dabei durchgängig auf HDTV umzustellen. Im Mittelpunkt steht die Investition in ein HDTV-fähiges Videospeichersystem und die Erneuerung der Sendeautomation. Parallel dazu hat der **rbb** die zugehörige Infrastruktur umgestellt, so dass alle HDTV Videosignale in Echtzeit verarbeitet werden können.
Die bisherigen Materialquellen der Sendeabwicklung wurden bei den Erneuerungen berücksichtigt. Die bestehenden Arbeitsabläufe in der Sendeabwicklung konnten weitgehend beibehalten werden.

Auch in diesem Bereich werden nur wenige personenbezogene Nutzerdaten verarbeitet. Für den Abschluss meiner Vorabkontrolle ist noch das Informationssicherheitskonzept erforderlich, das derzeit erstellt wird.

4. Dispositionssystem MIRAAN

Wie in meinem letzten Tätigkeitsbericht mitgeteilt, ist beim **rbb** Ende Jahr 2015 der Probebetrieb eines neuen Dispositionssystems gestartet. Es handelt sich um die Software MIRAAN, die bei HR und SWR bereits im Einsatz ist.

Inforadio und rbbI24 (ehemals rbb online) erstellen seit Ende 2015 ihre Dienstpläne mit MIRAAN. Aktuell implementiert der Hersteller die **rbb**-spezifischen Änderungsanforderungen. Parallel dazu wird derzeit im Detail im **rbb** geklärt, wie zukünftig mit MIRAAN gearbeitet werden soll. In diesen Klärungsprozess werden der Informationssicherheitsbeauftragte und ich mit einbezogen.

Die "rbb-Version" von MIRAAN soll Ende September ausgeliefert werden. Anschließend folgt eine einmonatige Testphase. Falls in dieser keine größeren Fehler gefunden werden, soll MIRAAN ab November in weiteren Bereichen eingeführt werden.

5. Software „Jira“ zum Fehlertracking

Seit 2006 setzen verschiedene Bereiche in der Produktions- und Betriebsdirektion die Software Jira ein. Dabei handelt es sich um eine Software zum Fehlertracking. Jira bietet Möglichkeiten, einen Auftrag an verschiedene Personen zur Bearbeitung weiterzuleiten und so jederzeit einen Gesamtüberblick über die zu bearbeitenden Vorgänge zu erhalten. Der Betrieb und die Administration erfolgen in der OUI. Nach Herstellerangaben ist die Software mit Auswertungsmöglichkeiten versehen.

Leider wurde seinerzeit bei Einführung des Systems versäumt, die Datenschutzbeauftragte einzubeziehen, so dass auch eine datenschutzrechtliche Vorabkontrolle des Systems bisher nicht stattfinden konnte. Erst im Frühjahr dieses Jahres habe ich von einem Mitarbeiter einen Hinweis auf die geplante Einführung im Technischen Programmservice erhalten. Der zuständige Abteilungsleiter hat mir auf Nachfrage einige Informationen über die geplante Anwendung gegeben und auch versichert, dass eine Verhaltens- und Leistungskontrolle der Mitarbeiterinnen und Mitarbeiter nicht stattfindet. Um die „Vorab“kontrolle des Systems nachholen zu können, benötige ich jedoch noch weitere Informationen. Wie ich von der Vorsitzenden des Personalrates erfahren habe, ist verabredet, dass bis November 2016 auch der Zustimmungsantrag zur Anwendung der Software mit allen erforderlichen Informationen einschließlich des Votums der Datenschutzbeauftragten dem Personalrat vorgelegt werden soll.

6. muPRO – Die multimediale Produktions-App

Seit Januar 2016 ist die neue multimediale Produktions-App im **rbb** im produktiven Einsatz. Die muPRO-App ermöglicht die Aufnahme, Bearbeitung und Übertragung von Audiobeiträgen mit einem Smartphone, Laptop oder normalem PC. Per ARD-Audiofiletransfer-System können die Beiträge an alle ARD-Anstalten sehr einfach übertragen werden. Dabei wird das Material an einen Server im ARD-Sternpunkt übermittelt und von dort an die sendende(n) Rundfunkanstalten „weitergeleitet“. Darüber hinausgehend sind mit der App aber auch qualitativ hochwertige Live-Audioverbindungen möglich. Voraussetzungen für den Einsatz sind geeignete Audi-

ohardware (Mikrofon, Kopfhörer) und eine schnelle Internetverbindung am Einsatzort.

Im Rahmen der Berichterstattung, für die die muPROApp genutzt wird, werden naturgemäß auch personenbezogene Daten in unterschiedlichem Ausmaß verarbeitet. Da diese Verarbeitung personenbezogener Daten im Regelfall ausschließlich zu eigenen journalistisch-redaktionellen Zwecken erfolgt, unterfällt der Sachverhalt dem sog. Medienprivileg. Gemäß § 36 Abs. 2 **rbb**-Staatsvertrag gelten neben den Bestimmungen des **rbb**-Staatsvertrages, nur einige wenige Vorschriften des Bundesdatenschutzgesetzes entsprechend. Im Wesentlichen handelt es sich dabei um Vorschriften zur Datensicherheit. Die Anmeldung der Nutzer erfolgt über einen beim ARD-Sternpunkt gehosteten Lizenzserver.

Seitens des **rbb** wird die IP – basierte (= Internetprotokoll, d. h. Übertragung basierend auf Internettechnik/über Internet) Übertragung der Daten in die einzelnen Rundfunkanstalten zentral über den ARD-Sternpunkt vorgenommen. Dabei wird der Dienst „Audio-over-IP" (AoIP) eingesetzt, der bereits im Jahre 2011 eingeführt worden ist, um eine Infrastruktur für das Absetzen von Audiobeiträgen über IP-Netzwerke bereitstellen zu können. Die dort implementierten Sicherheitsmaßnahmen zur Gewährleistung einer sicheren Übertragung sowie zur Absicherung des ARD-CN gegen das Internet wurden zum damaligen Zeitpunkt sowohl von externen Dienstleistern (sicherheitstechnische Überprüfung durch den TÜV Rheinland in 2010) als auch vom ARD-internen Informationssicherheitsgremium für das ARD-CN geprüft und als zuverlässig eingestuft. Insoweit ist die Gewährleistung der Datensicherheit auf Seiten des **rbb** sichergestellt.

Allerdings muss die Datensicherheit auf den von den Reportern verwendeten **rbb**-eigenen Geräten noch erhöht werden (s. C I 4.). Für die Nutzung der MuProApp auf Privatgeräten muss ebenfalls ein schlüssiges Datenschutz- und Informationssicherheitskonzept erarbeitet werden. Es ist derzeit in Arbeit.

Aus diesem Grund habe ich der Nutzung der MuProApp auf Dienstgeräten unter der Bedingung zugestimmt, dass bei den Datensicherheitsmaßnahmen nachgebessert

wird. Der Nutzung der MuProApp auf Privatgeräten kann ich demgegenüber erst zustimmen, wenn das Datenschutz- und Informationssicherheitskonzept vorliegt. Der Personalrat hat sich meinem Votum angeschlossen und der Einführung der MuProApp zunächst ebenfalls nur für Dienstgeräte zugestimmt.

7. Erstellung einer Cloud-Lösung für das Online-Ausspiel

Derzeit werden alle Server für das Ausspiel der Webauftritte des **rbb** intern betrieben. Die Systeme haben in 2016 zu einem Großteil das Ende ihres Lebenszyklus erreicht und müssen ersetzt werden. Zusätzlich müssen bei besonderen Events (Wahlen, Sportereignisse, etc.) immer größere Lastspitzen abgefangen werden. Zu einem überwiegenden Teil der Zeit wird jedoch nur ein Bruchteil der verfügbaren Systemleistung für das Standardausspiel benötigt. Aufgrund der stetig steigenden Nutzung der Webauftritte des **rbb** und deren wachsender technischer Komplexität, bindet die rein technische Wartung der Systeme in immer stärkeren Maße die internen Ressourcen der zuständigen **rbb** -Kollegen. Diese stehen dann für Support- und Projektarbeiten nur eingeschränkt zur Verfügung. Die Lösung dieses Problems wird darin gesehen, zusätzliche sog. Cache-Systeme in eine öffentliche Cloud zu stellen.

Unter Berücksichtigung der Tatsachen, dass die Inhalte, die im Rahmen dieses Projekts in die Cloud gestellt werden sollen, zur Veröffentlichung bestimmt sind und damit unter das Medienprivileg fallen, und dass beabsichtigt ist, mit einem deutschen zertifizierten Anbieter mit Servern in Deutschland zusammenzuarbeiten, habe ich dem Vorhaben grundsätzlich zugestimmt. Dabei habe ich darauf hingewiesen, dass mit dem Anbieter die Mustervereinbarung zur Auftragsdatenverarbeitung abgeschlossen werden muss.

8. Elektronische Formulare (eForm)

Seit September 2014 läuft die Anwendung ProcessFlow im **rbb** im Probebetrieb. Mit Hilfe dieser Workflow-Komponente von Lotus Notes können Formulare am Bildschirm ausgefüllt und anschließend in einem elektronischen Verfahren zur Genehmigung weitergeleitet werden. Im März 2015 haben sich Personalrat und OUI darauf verständigt, dass für jedes neue Formular in eForm zukünftig ein eigenständiger Zustimmungsantrag erforderlich ist. Dem Antrag auf Zustimmung an den Personalrat wird regelmäßig auch die Einschätzung der Datenschutzbeauftragten beigefügt.

Im September 2015 habe ich dem Formular für die Studentenvereinbarungen und im Oktober 2015 dem überarbeiteten Formular zum Einrichten, Ändern, Löschen von Benutzerkonten und –berechtigungen und Neueinstellungen eines PC-Arbeitsplatzes zugestimmt.

III. Beschäftigtendatenschutz

1. Fragen zur Auslegung des Berliner Datenschutzgesetzes beim Beschäftigtendatenschutz

Im Zusammenhang mit den Verhandlungen über die SAP-Dienstvereinbarungen ist vom Personalrat wiederholt die Frage nach den Rechtsgrundlagen für konkrete Datenverarbeitungen aufgeworfen worden. Da der Gesetzgeber bei Verabschiedung des Berliner Datenschutzgesetzes (BlnDSG) wohl eher eine typische Berliner Behörde als eine staatsunabhängige Rundfunkanstalt vor Augen hatte, sind die Vorschriften zum Teil nicht ganz eindeutig und müssen ausgelegt werden.

Um hier Klarheit zu erlangen und Diskussionen zwischen der externen Beraterin des Personalrats, dem Justitiariat und mir abzukürzen, habe ich mich im Sommer 2015 an den Berliner Beauftragte für Datenschutz und Informationssicherheit gewandt. Die für die Verarbeitung von wirtschaftlich-administrativen Daten zuständige Kontrollbehörde für den **rbb** bestätigte meine Rechtsauffassung und beantwortete die Anfrage wie folgt:

„1. Nach § 2 Abs. 2 BlnDSG i. V. m. § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Personaldatenverarbeitung zu Arbeitgeberzwecken wie z. B. für die Personalplanung und den Personaleinsatz werden nach unserem Dafürhalten grundsätzlich von der Vorschrift gedeckt. Allerdings haben sich Datenerhebung und –verarbeitung am Gebot der Erforderlichkeit zu orientieren. Keinesfalls darf weder die Personalplanung noch der Personaleinsatz als Generalermächtigung betrachtet werden, uferlos Personaldaten des Beschäftigten einzuholen und zu verwenden.

2. (...) Auch freie Mitarbeiterinnen und Mitarbeiter fallen unter die Vorschrift des § 2 Abs. 2 BlnDSG i. V. m. § 32 BDSG, sofern sie auf die Einkünfte aus der Dienstleistung zur Sicherung ihrer Existenzgrundlage angewiesen sind bzw. es sich nicht um kleine Aufträge handelt. Dies ist im Einzelfall zu prüfen. Alternativ könnte als Rechtsgrundlage die Generalklausel des § 6 Abs. 1 Satz 2 BlnDSG als Rechtsgrundlage herangezogen werden.“

Damit ist klar: Sofern die Datenverarbeitung betrieblich notwendig und verhältnismäßig ist, gibt es entsprechende gesetzliche Grundlagen und es bedarf keiner zusätzlichen Einwilligung der Mitarbeiterinnen und Mitarbeiter in die Datenverarbeitung.

2. Compliance im rbb

Seit Herbst 2015 gibt es im **rbb** eine neue Struktur, um regelgerechtes, ethisch korrektes Verhalten weiter zu unterstützen. Die Intendantin hat die stellvertretende Justitiarin Frau Dr. Kerstin Skiba zur (ehrenamtlichen) Compliance-Beauftragten ernannt. Diese wird durch ein „Ad –hoc-Beratungsgremium" unterstützt. Das Beratungsgremium tagt nicht regelmäßig, sondern kommt nur anlassbezogen zusammen. Dem Gremium gehören an: ein Mitglied der Personalabteilung, ein Vertreter der Revision und je nach Lage des aktuellen Falles Abgesandte aus der Produktions- und Betriebs- oder aus der Programmdirektion. Auch die Datenschutzbeauftragte wird bei Bedarf hinzugezogen. Meine Aufgabe ist es im Wesentlichen, die Möglichkeiten und Grenzen der Verarbeitung von Beschäftigtendaten zur Aufklärung etwaiger Straftaten im jeweiligen Einzelfall festzulegen.

Am 19. Februar 2016 hat das Gremium unter Vorsitz der Compliance-Beauftragten zum ersten Mal getagt, um allgemeine Fragen zur Zuständigkeit des Gremiums und zum Verfahren zu klären.

3. Bewerbermanagementsystem

Schon in meinem letzten Tätigkeitsbericht habe ich darüber berichtet, dass der **rbb** ein neues elektronisches Bewerbermanagementsystem einführen wird. Der Beginn des Probebetriebs hat sich wegen der Notwendigkeit der Klärung von Detailfragen (u. a. zum Datenschutz) weiter verzögert. Inzwischen konnten alle noch offenen Punkte geklärt werden. Der Probebetrieb soll nun im Herbst 2016 starten.

4. Konzeption und Erprobung einer strategischen Personalplanung

Am 18. November 2015 fand die erste Sitzung des Lenkungsausschusses des Projektes „Konzeption und Erprobung einer strategischen Personalplanung statt. Am 11. Januar 2016 erläuterten mir die beiden Projektleiter ihr Vorhaben. Kernfragen der strategischen Personalplanung sind:
Wie viele Mitarbeiterinnen und Mitarbeiter mit welchen Qualifikationen und in welcher Beschäftigungsform benötigt der **rbb** wann?
Wie kann der identifizierte Personalbedarf optimal quantitativ und qualitativ gedeckt werden?
Der Projektauftrag besteht in der Beschreibung eines handhabbaren und praxisorientierten Personalplanungsprozesses, der die strategische Personalplanung sowohl mit den Strategie- und Planungsprozessen des **rbb** als auch mit dem operativen Personalmanagement verknüpft.

Ich konnte den Projektleitern mitteilen, dass aus datenschutzrechtlicher Sicht nichts gegen das Konzept spricht. Personalplanung liegt im berechtigten Arbeitgeberinteresse. Die Rechtsgrundlage für die Verarbeitung von Mitarbeiterdaten zu diesem Zweck ergibt sich aus § 2 Abs. 2 BlnDSG i. V. m. § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz für festangestellte Mitarbeiterinnen und Mitarbeiter und für arbeitnehmerähnliche Personen und für alle sonstigen freien Mitarbeiter aus § 6 Abs. 1 Satz 2 BlnDSG. Die geplante Datenverarbeitung ist auch verhältnismäßig.

Ich habe die Projektleiter darum gebeten, mit mir alle organisatorischen Fragen wie Datenkatalog, Berechtigungskonzept, Aufbewahrungsfristen etc. zu klären, bevor das Projekt in die Regelstruktur übergeht.

5. Neuer Arbeitsplan im Bereich der Programmdokumentation

Im November 2015 ist der Bereichsleiter der Programmdokumentation auf mich zugekommen und hat mir seine Idee für einen neuen Arbeitsplan im Bereich der Programmdokumentation erläutert. Der Plan soll als Exel-Tabelle angelegt werden

und sowohl zur Disposition als auch zu Planungs- und Steuerungszwecken durch die Bereichsleitung dienen. Unter anderem sind folgende Auswertungen geplant:

- Anzahl der verschiedenen Aufgabentage in der Programmdokumentation gesamt,
- Anzahl der Einsätze von externen Mitarbeitern in der Programmdokumentation,
- Anzahl Tage der Projektarbeit,
- Anzahl bestimmter Schichten und
- Anzahl der Azubis in den verschiedenen Gewerken.

Den Mitarbeitern, die lesenden Zugriff erhalten, soll – da technisch nicht verhinderbar - ausdrücklich verboten werden, Art und Anzahl der Einsätze sowie Abwesenheitszeiten ihrer Kolleginnen und Kollegen systematisch auszuwerten. Ferner soll es – mit Ausnahme der eigenen Einsätze – nicht gestattet sein, lokale Kopien der Arbeitsplan-Datei anzufertigen oder diese unbefugten Personen zugänglich zu machen. Die Nutzung des Bemerkungsfeldes soll nur für konkret festgelegte Bemerkungen wie Sitzungs- und Veranstaltungstermine und Datenbankausfälle durch Wartungsfenster genutzt werden. Personenbezogene Einträge sollen darin nicht vorgenommen werden.

Der Arbeitsplan wird nicht zur Auswertung von Abwesenheiten verwendet. Eine Leistungs- und Verhaltenskontrolle ist ebenfalls ausgeschlossen.

Der Arbeitsplan soll zunächst in einem zwei- bis dreimonatigen Probebetrieb erprobt werden. Ich habe dem Bereichsleiter mitgeteilt, dass ich die von ihm geplanten Auswertungen zu Planungszwecken als von § 2 Abs. 1 BlnDSG i. V. m. § 32 BDSG gedeckt ansehe. Derzeit befindet sich der Bereichsleiter noch in der Abstimmung mit dem Personalrat über das beabsichtigte neue Arbeitsmittel. Ein Probebetrieb hat noch nicht stattgefunden.

6. Versand elektronischer Gehaltsabrechnungen

In meinem letzten Tätigkeitsbericht hatte ich mitgeteilt, dass es innerhalb der Personalabteilung Überlegungen gibt, die Gehaltsabrechnungen künftig elektronisch zu versenden. Ich unterstütze diese Überlegungen. Aus meiner Sicht stellt die elektronische Versendung der Gehaltsabrechnungen unter Einhaltung entsprechender Sicherheitsmaßnahmen eine Verbesserung zur bisherigen Versendung per Hauspost dar. Im Berichtszeitraum hat eine kleine Arbeitsgruppe aus Vertretern der Personalabteilung, des IVZ, OUI, der Revision und mir ein Konzept für die elektronische Versendung der Dokumente erarbeitet. Dieses muss nun noch vom Informationssicherheitsbeauftragten freigegeben werden.

7. Registrierung der Ein- und Ausfahrten ins rbb-Parkhaus

Ausgelöst durch die Anfrage eines Kollegen zur Registrierung der Ein- und Ausfahrten ins/aus dem **rbb**-Parkhaus wurde nach einer Besprechung der aktuellen Verfahrensweisen folgendes Vorgehen mit der Abteilung Infrastruktur besprochen:

In einer Liste werden täglich Lieferanten und Dienstleistungsfirmen registriert, die eine temporäre Zufahrtsgenehmigung für das **rbb**-Gelände erhalten und deren Verlassen des Geländes vom Wachschutz kontrolliert wird. Diese Registrierung wird beibehalten.

Für die Überprüfung der Berechtigungen der ins Parkhaus einfahrenden Fahrzeuge sollen statt des Notierens von Kennzeichen beim Einfahren in das Parkhaus die Berechtigungen nach Möglichkeit durch den Wachschutz kontrolliert werden. Zulässig ist auch eine stichprobenartige Kontrolle, welche Fahrzeuge im Parkhaus stehen, wenn die dabei erstellten Notizen keine Ein- und Ausfahrtzeit, sondern nur die vorgefundenen Kennzeichen zum Zeitpunkt X enthalten.

Aus meiner Sicht verdeutlich auch dieses Verfahren (, das nur eine Übergangslösung sein kann), wie dringlich die Umsetzung des inzwischen erstellten Sicherheits-

konzepts für die Zutrittsbedingungen und Schließsysteme/ Schlüsselverwaltung im **rbb** insgesamt ist (s. C I 3.).

8. Transponder-Türschließ-System im Bereich technischer Programmservice

Im März 2016 hat sich der Personalrat an den Leiter des Technischen Programmservice gewandt, weil er erfahren hatte, dass in diesem Bereich seit längerem ein elektronisches Öffnungs- und Zutrittssystem genutzt wird, das prinzipiell auch zur Zeiterfassung genutzt werden könnte. Da vor Einführung dieses Systems kein Beteiligungsverfahren durchgeführt worden war, bat der Personalrat um Information. Ich erhielt von dem entsprechenden Schreiben eine Kopie. Der Bereichsleiter versicherte uns, dass in dem System keine personenbezogenen Daten hinterlegt sind. Dadurch ist keine Zuordnung der Transponder zu einzelnen Mitarbeitern möglich.

9. Datenschutzprüfung der Beihilfe- und Bezüge-Zentrum GmbH

Am 24. Juni 2015 haben die Datenschutzbeauftragten von BR, SWR, NDR und ZDF stellvertretend für alle betroffenen Datenschutzbeauftragten die Abwicklung der Beihilfe-Berechnungen für Mitarbeiterinnen und Mitarbeiter der Rundfunkanstalten durch das Beihilfe- und Bezüge-Zentrum GmbH (bbz) vor Ort in Bad Dürkheim geprüft. Die bbz berechnet die Beihilfe auch im Auftrag des **rbb**.

Wegen ihrer Verantwortung für die datenschutzgemäße Behandlung von Mitarbeiterdaten auch im Falle der Verarbeitung durch Externe und aufgrund der Sensibilität der betroffenen Daten prüfen die Rundfunkdatenschutzbeauftragten die bbz GmbH regelmäßig. Die bbz führt die Berechnungen für die Mitarbeiter der Anstalten im Rahmen einer Auftragsdatenverarbeitung durch. Die bbz hat einen betrieblichen Datenschutzbeauftragten, der anlässlich der Prüfung für Fragen und Erläuterungen zur Verfügung stand. Bei ihm waren im zu prüfenden Zeitraum weder Auskunftsersuchen noch Datenschutzbeschwerden eingegangen.

10. Datenverarbeitung bei der Baden-Badener Pensionskasse

Der **rbb** hat – wie auch alle anderen Landesrundfunkanstalten – die Baden-Badener Pensionskasse (bbp) – einen Versicherungsverein auf Gegenseitigkeit – mit der Abwicklung der Versorgungsleistungen nach dem Versorgungstarifvertrag beauftragt und eine entsprechende Vereinbarung über Auftragsdatenverarbeitung mit der bbp abgeschlossen. Der Sitz der bbp befindet sich in den Räumlichkeiten des SWR in Baden-Baden. Die Arbeitsplätze sind an das Kommunikationsnetz des SWR angebunden.

Zum 1. Juli 2014 hat – wie im letzten Tätigkeitsbericht erwähnt – das IVZ am Standort Köln das Hosting für die bbp übernommen. Zur Rechtsstellung des IVZ s. E. Erst im Herbst 2015 konnten die Datenschutzbeauftragten der Rundfunkanstalten das Sicherheitskonzept für das Hosting freigeben. In Ergänzung dazu fand am 20. Oktober 2015 ein Gespräch beim IVZ in Köln statt, an dem neben der Geschäftsleitung der bbp, verschiedene Mitarbeiter des IVZ sowie die Datenschutzbeauftragten von NDR, SWR und **rbb** sowie die Informationssicherheitsbeauftragte des MDR teilnahmen. In diesem Gespräch konnten letzte, noch offene Fragen zur Informationssicherheit beim Hosting durch das IVZ geklärt werden. Außerdem wurden auch andere datenschutzrechtliche Aspekte bei der bbp behandelt. So sollen u. a. die Arbeitgeberportale, also die Verbindung zu den einzelnen Rundfunkanstalten und deren Tochtergesellschaften, durch verschärfte Passwortrichtlinien eine erhöhte Sicherheit erfahren, die Verträge mit Softwareherstellern zur Bestandsverwaltung und für steuerliche und krankenversicherungstechnische Berechnungen auf die Erfüllung der datenschutzrechtlichen Vorgaben zur Auftragsdatenverarbeitung überprüft werden und die USB-Anschlüsse der Arbeitsplätze in Baden-Baden restriktiver gehandhabt werden.

11. Datenschutzrechtliche Aspekte bei der Auslegung des Freienstatuts

Wie in meinem letzten Tätigkeitsbericht erwähnt, ist zum 1. Juni 2014 das Freienstatut in Kraft getreten. Darin sind u. a. die Modalitäten der Wahl und die Pflichten der Freienvertretung und ihrer Mitglieder geregelt. Aus datenschutzrecht-

licher Sicht sind insbesondere die in dem Statut geregelten Auskunfts- und Informationsrechte relevant. Wiederholt hat sich die Freienvertretung im Berichtszeitraum an die Personalabteilung gewendet und um umfangreiches Datenmaterial gebeten, das aus ihrer Sicht zur Erfüllung ihrer Aufgaben nach dem Freienstatut erforderlich sei. In Abgrenzungsfragen hat mich die Personalabteilung jeweils hinzugezogen. Unter anderem ging es dabei um die Frage, ob die Freienvertretung – analog zur Personalvertretung – einen Bestand an personenbezogenen Grunddaten der arbeitnehmerähnlichen Personen dauerhaft speichern darf.

Die Aufgaben und Informationsrechte der Freienvertretung (§§ 34, 36 Freienstatut) ähneln den entsprechenden Regelungen im Bundespersonalvertretungsgesetz (§§ 67,68 BPersVG). Allerdings gibt es auch wichtige Unterschiede:

- Das Freienstatut hat keine Gesetzesqualität.
- Im Freienstatut wird - anders als im BPersVG - die Unterrichtungspflicht in § 36 Abs. 2 Satz 2 durch die Aufzählung einzelner Auskunftspflichten konkretisiert. Zwar ist diese Aufzählung nicht abschließend ("... insbesondere...."), sie schränkt aber den Informationsanspruch gegenüber dem in § 68 BPersVG ein und man kann mindestens für die genannten Regelbeispiele aus dem Wortlaut Schlüsse ziehen. Aus der Formulierung "*Zahlen* zur Beschäftigung arbeitnehmerähnlicher Personen..." folgt etwa, dass die Verfasser des Statuts in diesem Kontext die Nennung von personenbezogenen bzw. -beziehbaren Daten gerade nicht beabsichtigt haben.

Des Weiteren gilt: Es ist nicht die Aufgabe der Freienvertretung – ebenso wenig wie die des Personalrats -, die Aufgabenerfüllung und den inneren Betrieb des **rbb** allgemein und unabhängig von den ihr zugewiesenen Aufgaben zu überwachen. Die Freienvertretung kann daher - wie der Personalrat - Informationen seitens der Dienststelle nur aus einem bestimmten Anlass und in Bezug auf eine konkrete ihr nach dem Gesetz obliegende Aufgabe verlangen. Kurz gefasst: Es besteht kein ganz allgemeiner und übergreifender Informationsanspruch.

Andererseits benötigt die Freienvertretung – wie der Personalrat – einen Grundbestand an Daten ihrer Klientel für ihre Arbeit.

Zur Ermittlung der erforderlichen Daten hat die Personalabteilung in meinem Beisein mehreren Gesprächen mit der Freienvertretung, geführt. Danach halte ich die halbjährliche Übermittlung einer Liste mit allen arbeitnehmerähnlichen Personen zum jeweiligen Stichtag mit folgenden Angaben für zulässig:

- Name, Alter, überwiegend ausgeübte Tätigkeit.

Nach wie vor nicht nachvollziehbar ist für mich, wofür die Freienvertretung die ebenfalls geforderte Angabe "erstmalige Beschäftigung" aller arbeitnehmerähnlichen Personen benötigt. Denn aus diesem Datum allein können keinerlei Rechte für die freien Mitarbeiterinnen und Mitarbeiter abgeleitet werden. Aus meiner Sicht besteht auch kein Anspruch auf eine Übermittlung sämtlicher Honorardaten aller arbeitnehmerähnlichen Personen.

Sollten die Freienvertretung im Einzelfall Anhaltspunkte für Unregelmäßigkeiten bzw. eine Diskriminierung im Zusammenhang mit der Zahlung von Honoraren haben, so besteht in dem konkreten Fall ein Anspruch auf Einblick in die entsprechenden Akten bei der Personalabteilung.

Darüber hinaus bestehen aus datenschutzrechtlicher Sicht keine Einwände gegen die Übermittlung von anonymen bzw. pseudonymen Daten für statistische Auswertungszwecke.

Die Freienvertretung hat sich im Dezember 2015 an den Berliner Beauftragten für Datenschutz und Informationsfreiheit mit der Bitte um eine rechtliche Einschätzung gewandt. Die für Beschäftigtendatenverarbeitung bei der Behörde zuständige Sachbearbeiterin teilt im Wesentlichen meine Auffassung. Es gibt lediglich einige

wenige Abweichungen hinsichtlich des Datenkatalogs, der der Freienvertretung regelmäßig zur Verfügung gestellt werden muss. Die Kollegin vom Berliner Datenschutz hat der Freienvertretung bescheinigt, dass auch auf die Mitteilung des Beginn des Rechtsverhältnisses, die ausgeübte Funktion und die tarifliche Bewertung ein Anspruch besteht. Dabei hat sie aber meiner Ansicht nach wohl zum einen übersehen, dass die freien Mitarbeiterinnen und Mitarbeiter – anders als Angestellte und Beamte - aus dem Datum der erstmaligen Beschäftigung allein keinerlei Ansprüche ableiten können und dass die freien Mitarbeiterinnen und Mitarbeiter regelmäßig sehr unterschiedliche Funktionen mit unterschiedlichen tarifvertraglichen Bewertungen ausüben. Insofern sehe ich derzeit keinen Anlass, meinen Standpunkt zu überdenken.

12. Überarbeitung der Fragebögen für freie Mitarbeiterinnen und Mitarbeiter

Wie in meinem letzten Tätigkeitsbericht angekündigt, habe ich im Herbst 2015 zusammen mit der Personalabteilung die Fragebögen für freie Mitarbeiterinnen und Mitarbeiter überarbeitet. Dabei konnten zahlreiche Datenfelder gestrichen werden, weil unsere Prüfung ergeben hatte, dass die bislang erhobenen personenbezogenen Daten zum Teil gar nicht benötigt werden. Der Verwendungszweck der Daten ist nun klarer definiert. Außerdem ist die Information über die Datenverwendung jetzt verständlicher.

13. Honorardatenabgleich zwischen den Rundfunkastalten

Im Zuge der Überarbeitung der Fragebögen für freie Mitarbeiter stellte sich für mich die Frage nach der Notwendigkeit eines seit vielen Jahren geübten Honorardatenabgleichs zwischen den Personalabteilungen der Rundfunkanstalten. Bis dahin hatten die Personalabteilungen einmal jährlich Namen und Verdiensthöhen von freien Mitarbeiterinnen und Mitarbeitern ausgetauscht, von der sie durch die Angabe der betreffenden Mitarbeiterinnen und Mitarbeiter wussten, dass sie bei einer anderen ARD-Anstalt fest angestellt sind.

Für diesen umfangreichen Datenaustausch, insbesondere über die Höhe der Einkünfte, sah ich nach genauerer Prüfung keine Rechtsgrundlage und letztlich auch keine Notwendigkeit.

Aus meiner Sicht hat der **rbb** lediglich ein berechtigtes Informationsinteresse daran zu erfahren, ob jemand Arbeitnehmer oder Versorgungsempfänger einer anderen Rundfunkanstalt ist. Denn in diesem Fall hat der freie Mitarbeiter /die freie Mitarbeiterin nach den rbb-Honorarrichtlinien nur einen Anspruch auf 50% des Honorars.

Anfang 2016 hat der **rbb** auf meine Bitte erstmalig von der Praxis der Datenübermittlung der Honorarhöhen abgesehen. Auf die Einstellung der Datenlieferung gab es keine Reaktionen aus den anderen Rundfunkanstalten.

14. Musiktiteleinsatzkontrolle und GEMA-Listen

Auf Anregung der Revision hat im Sommer 2015 eine kleine Arbeitsgruppe unter der Leitung der OUI damit begonnen, ein Verfahren zu entwickeln, mit dem die Einhaltung des grundsätzlichen Verbots für Musikredakteure, ihre eigenen GEMA-pflichtigen Titel einzusetzen, sichergestellt werden kann. Anders als in einigen anderen Rundfunkanstalten existiert beim **rbb** bislang keine entsprechende Regelung. Auf Nachfrage habe ich der Arbeitsgruppe die zu berücksichtigenden datenschutzrechtlichen Aspekte erläutert. Dabei gilt es, einen sachgerechten Ausgleich zwischen dem Recht auf Datenschutz der Mitarbeiterinnen und Mitarbeiter und den berechtigten Kontrollinteressen des **rbb** zu schaffen. Wichtig ist auch die transparente Ausgestaltung des Verfahrens.

In diesem Zusammenhang habe ich von einem seit den 70er Jahren im Auftrag der Intendanten praktizierten Datenaustausch zwischen der im Auftrag aller Landesrundfunkanstalten handelnden SWR-Revision und der GEMA erfahren. Zu diesem Zweck hatten die Landesrundfunkanstalten – soweit bekannt - der SWR-Revision die Namen ihrer Mitarbeiterinnen und Mitarbeiter mit GEMA-pflichtigen Werken mitgeteilt. Die SWR-Revision hatte diese Daten an die GEMA weitergeleitet mit dem Ziel

zu erfahren, ob und in welcher Höhe an diese Mitarbeiter Tantiemen infolge des Einsatzes eigener Musikwerke ausgezahlt wurden. Inzwischen hat die GEMA die Information an die Rundfunkanstalten aus Datenschutzgründen eingestellt. Daraufhin haben alle Rundfunkanstalten ihre Datenübermittlungen an die SWR-Revision eingestellt.

Ich halte die Entscheidung der GEMA für korrekt. Die Kontrolle aller Musiktiteleinsätze war unverhältnismäßig. Stichprobenhafte Kontrollen auf der Grundlage einer klaren Regelung halte ich hingegen für zulässig. Eine derartige Regelung ist im **rbb** noch nicht getroffen, da man zunächst die Entwicklungen auf ARD-Ebene abwarten wollte.

15. Erhebung von Mitarbeiterdaten für die Erstellung ins Journalistenverzeichnisses für PR-Kunden

Anfang 2016 wandte sich der Redakteursausschuss mit der Bitte um Unterstützung an das Justitiariat. Ein Unternehmen mit Firmensitz in Frankfurt a.M sammle offenbar gezielt Daten von festen und freien **rbb**-Journalisten für die Erstellung eines Journalistenverzeichnisses für PR-Kunden. Viele Kolleginnen und Kollegen seien von dem Unternehmen angeschrieben worden. Für den Fall, dass man nicht aktiv widerspreche, lande man automatisch in dieser Datenbank. Das Justitiariat hat die Sache an mich zur Bearbeitung abgegeben. Ich habe mich mit dem Unternehmen in Verbindung gesetzt, um zu erfahren, aus welchen Quellen die dienstlichen E-Mail-Adressen und Informationen über die dienstlichen Funktionen der Mitarbeiterinnen und Mitarbeiter stammen, welche konkreten personenbezogenen Daten gespeichert werden und auf welcher Rechtsgrundlage die Daten erhoben und weiterverarbeiten werden. Ich erhielt die Antwort, dass das Unternehmen "ein internationales Medien- und Journalistenverzeichnis, das von PR-Kunden weltweit genutzt wird, um so ihre Pressekontakte zu managen" habe. Bei den gespeicherten Daten handle "es sich ausschließlich um professionelle Daten wie Email-Adresse, Telefonnummer, Adresse und die Sektoren, die der jeweilige Journalist abdeckt." Diese Informationen dienten ausschließlich dem Ziel, "Pressekontakten die Mittel zu

geben, zielgerichtete Pressemitteilungen zu versenden." Die Daten seien durch eine öffentlich zugängliche Internet-Recherche, Anrufe bei der Publikation oder ein direktes Gespräch mit dem Journalisten erhoben.

Ich teilte dem Redakteursausschuss mit, dass - falls dem tatsächlich so ist - die Speicherung der beruflichen Daten der Kolleginnen und Kollegen zunächst grundsätzlich nach § 29 Abs. 1 S. 2 i.V.m. § 28 Abs. 3 S. 2 Nr. 2 Bundesdatenschutzgesetz (BDSG) zulässig sei. Nach § 29 Abs. 1 BDSG ist das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, unter bestimmten Voraussetzungen zulässig. Dabei umfasst Werbung nicht nur das Anpreisen von Waren oder Dienstleistungen. Es können vielmehr auch soziale, gesellschaftliche, ideelle oder politische Ziele beworben werden. Leider sieht das Gesetz in einem solchen Fall lediglich eine sog. "Opt-out"-Lösung vor, d.h. der Betroffene selbst muss sich gegen die Speicherung seiner Daten wehren. Hierzu genügt ein Widerspruch hinsichtlich der Nutzung, Speicherung und Übermittlung der eigenen personenbezogenen Daten. Dieser Widerspruch muss dabei vom Betroffenen selbst ausgesprochen werden. Der **rbb** kann gegen die Verarbeitung der Daten seiner Beschäftigten dagegen nicht vorgehen. Sollte das Unternehmen hingegen auf unrechtmäßigem Weg an die Daten herangekommen sein, so wäre natürlich auch die Datenverarbeitung an sich illegal.

Ich habe – in Abstimmung mit einem Mitarbeiter des hessischen Landesdatenschutzbeauftragten - vorgeschlagen, dass die betroffenen Journalistinnen und Journalisten zunächst ihren nach dem BDSG bestehenden Auskunftsanspruch gegenüber dem Unternehmen geltend machen. Dieser umfasst auch ein Recht auf Auskunft darüber, aus welcher Quelle die Daten konkret stammen. Zu diesem Zweck habe ich ein entsprechendes Anschreiben für die Journalisten entworfen. Außerdem habe ich darauf hingewiesen, dass die Betroffenen sich mit einer Beschwerde an den hessischen Landesdatenschutzbeauftragten wenden könnten, sofern sich aus den Antworten auf den geltend gemachten Auskunftsanspruch der Verdacht erhärtet, dass die Daten illegal erlangt wurden.

IV. Datenschutz im Programm

1. Smart-TV

Wie in meinem letztjährigen Tätigkeitsbericht berichtet, haben die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten gemeinsam mit den Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich im Mai 2014 ein gemeinsames Positionspapier zu Datenschutzfragen bei Smart-TV veröffentlicht. Danach muss die anonyme Nutzung von Fernsehangeboten auch bei Nutzung eines Smart-TVs gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

Zusammen mit dem Datenschutzbeauftragten des Mitteldeutschen Rundfunks Stephan Schwarze hatte ich seinerzeit mit dem ARD-Playout-Center (POC) ein Verfahren beim Aktivieren der ARD-Startleiste bei HbbTV entwickelt, das den Datenschutz unter Berücksichtigung des heutigen Standes der Technik bestmöglich gewährleistet. Allerdings lässt sich dabei nicht vermeiden, dass zur Bereitstellung der HbbTV-Angebote über das Internet die IP-Adresse des Zuschauers auf den Webserver übertragen wird. Die von allen Rundfunkveranstaltern geübte Praxis, über eine mit dem Rundfunksignal versandte URL bereits bei Auswahl eines Senders unmittelbar und ohne weiteres Zutun der Nutzenden eine Internetverbindung zu dem Server des HbbTV –Anbieters auszulösen, wird von den staatlichen Datenschutzbeauftragten kritisiert. Der Aufruf der Web-Dienste im Rahmen von HbbTV und die damit einhergehende wechselseitige Kommunikation mit dem Anbieter dürfe nach ihrer Auffassung erst dann stattfinden, wenn dies durch die Nutzenden selbst initiiert wird. Dies könne z. B. durch die aktive Entscheidung erfolgen, den „Red-Button“ bei HbbTV zu betätigen und damit den Abruf eines Telemediendienstes bewusst zu veranlassen. In einem Gespräch am 15. September 2015 erläuterten mein Kollege vom MDR und ich dem seinerzeitigen Landesdatenschutzbeauftragten von Berlin, Herrn Dr. Dix, unsere Position: Der Anschluss eines Smart-TV an das Internet erfolge immer aktiv durch den Nutzer. Dabei dürfte jeder Nutzerin/jedem Nutzer bewusst sein, dass zur Übertragung erster Informationen an den Browser unmittelbar

nach Einschalten des Programms die IP-Adresse des Nutzers an den Anbieter übertragen werden muss. Es ist von einer stillschweigenden Einwilligung in die Übertragung der IP-Adresse auszugehen. Wer dies nicht wünscht, muss das Fernsehgerät vom Internet trennen bzw. die Internetfunktionalität des Gerätes ausschalten. Die Umstellung auf ein Verfahren, bei dem erst nach dem Drücken des Red Button eine Verbindung zum Internet aufgebaut wird und die IP-Adresse des Nutzers fliest, würde überdies technisch auf erhebliche Schwierigkeiten stoßen, die von den Rundfunkanbietern allein nicht behoben werden können.

Der „Düsseldorfer Kreis" (das Koordinationsgremium der obersten Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich) hat auf seiner Sitzung am 15./16.September 2015 eine Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste verabschiedet. Darin findet sich die Kritik an dem Aufbau der Verbindung zum Internet vor dem Drücken des Red Buttons wieder. Die Aufsichtsbehörden haben die Rundfunkanstalten aufgefordert, auf die übrigen beteiligten Instanzen (z. B. Standardisierungsgremien, Anbieter von Übertragungswegen und Gerätehersteller) einzuwirken, damit diese ihrerseits die notwendigen Voraussetzungen dafür schaffen, dass der Aufbau einer Internetverbindung vor Inanspruchnahme des interaktiven Teils des HbbTV-Angebots zukünftig unterbleiben kann. Für eine Übergangszeit sei ein beanstandungsfreier Betrieb von bestehenden HbbTV-Angeboten möglich, wenn dabei folgende Mindestanforderungen erfüllt werden:

- Vor dem Drücken des „Red Button" im Zusammenhang mit dem Einschalten eines HbbTV-Senders übertragene Nutzungsdaten werden nicht für die Bildung von Nutzerprofilen verwendet.
- Nach dem Drücken des „Red-Button" werden den Nutzenden leicht zugängliche, allgemeinverständliche Informationen über die Verarbeitung ihrer Nutzungsdaten zur Verfügung gestellt, in deren Rahmen sie auch über ihr Widerspruchsrecht gegen die Erstellung von Nutzungsprofilen informiert werden.

- Die Bildung von Nutzungsprofilen nach § 15 Abs. 3 Telemediengesetz (TMG) erfolgt frühestens nach einer Interaktion des Nutzenden mit dem interaktiven Teil des HbbTV-Angebots (Drücken des „Red Button“).
- Nutzende können der Profilbildung, wie in § 15 Abs. 3 TMG vorgesehen, in einfacher Form widersprechen. Durch Nutzende erklärte Widersprüche werden von den Anbietern unverzüglich umgesetzt.

Diese Anforderungen entsprechen demjenigen, was mein Kollege vom MDR und ich als Anforderungen definiert hatten. Der Berliner Datenschutzbeauftragte hat uns in diesem Zusammenhang schriftlich bescheinigt, dass die Praxis der ARD den Anforderungen entspricht. Dies haben die Beteiligten in der ARD natürlich erfreut zur Kenntnis genommen, wenngleich klar ist, dass die staatlichen Datenschutzbeauftragten für die Landesrundfunkanstalten der ARD überhaupt nicht bzw. jedenfalls nicht für den journalistisch-redaktionellen Bereich (diese Einschränkung betrifft Radio Bremen, den Hessischen Rundfunk und den **rbb**) zuständig sind. Hier obliegt die Kontrollkompetenz allein den Rundfunkdatenschutzbeauftragten.

Zwischenzeitlich haben sich die Datenschutzbeauftragten der ARD mit der Frage beschäftigt, ob wir im Lichte der neuen DS-GVO an unserer Auffassung festhalten können, wonach eine ausdrückliche Zustimmung der Nutzerinnen und Nutzer, die das Gerät mit dem Internet verbunden haben, zur Übertragung der IP-Adresse nicht erforderlich ist. Dies haben wir bejaht. Insofern sehen wir die beabsichtigte technische Änderung, wonach im Installationsprozess einiger fabrikneuer Smart-TV-Geräte zukünftig ausdrücklich ein Schritt vorgesehen werden soll, mit dem sich die Nutzerinnen/Nutzer mit dem „Einschalten“ der HbbTV-Funktion und der damit einhergehenden Übertragung personenbezogener Daten über das Internet ausdrücklich einverstanden erklären müssen, als rechtlich nicht unbedingt notwendige, aber sinnvolle Ergänzung an. Denn mit diesem Verfahren ist nun auch sichergestellt, dass Art. 13 der DS-GVO mit der Verpflichtung zur Information bei der Datenerhebung hinreichend Rechnung getragen wird.

2. Personalisierungskonzept für die ARD-Mediathek

Derzeit wird ein Personalisierungskonzept von ARD Online (ARD Onlinekoordination/ARD.de) für die ARD-Mediathek erarbeitet. Allen interessierten Nutzerinnen und Nutzern soll es dadurch künftig ermöglicht werden, aus dem gesamten Angebot der ARD-Mediatheken individuell auf Video- und Audiobeiträge zuzugreifen. Dafür sollen Personalisierungsfunktionen geschaffen werden, die die Nutzerinnen und Nutzer in die Lage versetzen, zielgerichtet und schnell auf Angebote zuzugreifen, die ihren Interessen entsprechen. Hier wird beispielsweise an Favoriten-, Merk- und Playlisten, Empfehlungen, Push-Nachrichten, Social- Media- Einbindungen gedacht. Die Personalisierungsfunktionen sollen dabei dem ausschließlichen Zweck dienen, ein konsistentes und nutzungsfreundliches Angebot über alle Plattformen hinweg zu schaffen.

Für die Nutzung des Angebots ist die Verwendung eines Klarnamens nicht erforderlich. Es ist ausreichend, wenn die Registrierung mittels eines Pseudonyms erfolgt. Damit wird den Vorgaben des Telemediengesetzes genügt.

Auf die Daten der Nutzerinnen und Nutzer soll nur insoweit zugegriffen werden, als dies für die spezifischen Angebote notwendig, redaktionell intendiert und vom Nutzer gewollt ist. Für den Nutzer entstehen keinerlei zusätzliche Kosten. Die Daten werden nicht zu kommerziellen Zwecken genutzt, selbstverständlich ist auch der Handel mit Daten ausgeschlossen. Den Nutzerinnen und Nutzern steht es zudem jederzeit frei, sich von Personalisierungsfunktionen und optionalen Nutzungsmessungen auch wieder abzumelden.

Die Grundsätze für eine personalisierte ARD-Mediathek werden für die Nutzerinnen und Nutzer transparent dargestellt und sind jederzeit einsehbar. Als Vorbild dient dabei die „Privacy Policy“ der BBC (vgl. folgenden Link http://www.bbc.com/privacy/information/policy/).

Der Entwurf eines entsprechenden Personalisierungskonzeptes ist dem Arbeitskreis der Datenschutzbeauftragten der ARD schon im Laufe des Jahres 2014 zur Prü-

fung vorgelegt worden und hat grundsätzliche Zustimmung gefunden. Der Prozess der Einarbeitung entsprechender Änderungs- und Ergänzungsvorschläge dauert noch an.

3. E-Mail an Teilnehmer des Fuchsprojekts

Im Jahr 2015 hat der **rbb** ein multimediales Projekt „Füchse in der Stadt" in Zusammenarbeit mit dem Leibniz Institut für Zoo- und Wildtierforschung gestartet. Die Zuschauerinnen und Zuschauer waren aufgefordert, dem **rbb** selbst erstellte Fotos und Videos mit Füchsen zuzusenden. Das Einverständnis zur Verwendung der E-Mail-Adresse war auf das Projekt begrenzt gewesen.

Im Oktober 2015 schickte die Projektleitung an die E-Mail-Adressen aller Teilnehmer Einladungen zu einem Herbstfest des Leibnitz-Instituts für Zoo- und Wildtierforschung (IZW). Dabei war versehentlich der gesamte E-Mail-Verteiler war für alle Adressaten sichtbar.

Daraufhin gab es einige Beschwerden: Nur manche richteten sich auch gegen die Zusendung der Einladung an sich. Alle Beschwerdeführerinnen und –führer bemängelten den sichtbaren Verteiler.

Ich habe dazu mit der Redaktionsleitung ein ausführliches Gespräch geführt. Dabei habe ich deutlich gemacht, dass es für die Verwendung von Kontaktdaten für andere Zwecke als für den ursprünglichen Zweck einer speziellen Einwilligung bedurft hätte. Bei der Versendung von Mail an einen großen Verteiler muss selbstverständlich mit mehr Sorgfalt gearbeitet werden. Die Redaktion hat zugesagt, diese Hinweise ernst zu nehmen. Bei Mails an einen großen Verteiler soll künftig nach dem 4-Augenprinzip verfahren werden.

4. Ausspielung der Online-Angebote über die Firmen G&L/Akamai

Auf der Basis eines Rahmenvertrages, den der WDR für die ARD und ZDF vor einigen Jahren geschlossen hat, arbeitet auch der **rbb** mit den Firmen Geißendörfer &

Leschinsky (G&L) GmbH/Akamai zusammen, um seine Video- und Audiofiles in den Online-Angeboten zur Verfügung zu stellen und auch das Live-Streaming des **rbb**-Fernsehens, der Radiowellen sowie größerer Sport- und Kulturereignisse bereitzustellen. Akamai bietet dafür die technische Plattform, Betrieb und Support der Streams erfolgt über G&L. Problem dabei: Akamai hat seinen Hauptsitz in den USA. Auch die Server von Akamai stehen unter anderem in den USA.

Vor dem Hintergrund des EuGH-Urteils zu Safe Harbor (s. B I 2.), hat der WDR – in Abstimmung mit der Kollegin beim WDR und den anderen Datenschützern von ARD und ZDF- mit G&L/Akamai inzwischen nachverhandelt und in Ergänzung zu dem bestehenden Vertrag die EU-Standardvertragsklauseln abgeschlossen. Damit ist die ARD zunächst auf der formalrechtlich sicheren Seite.

Für die Zukunft muss sie aus meiner Sicht aber eine Lösung anstreben, bei der die Server in Europa stehen und Zugriffsrechte der US-Ermittlungsbehörden ausgeschlossen sind.

5. Mobile App rrb 24

Apps sind Anwendungssoftware für mobile Endgeräte (Smartphone, Tablet) und stationäre Geräte (Smart-TV, Apple-TV u.ä.). Sie können Daten in großem Umfang erfassen und verarbeiten, um dem App-Nutzer neue und innovative Dienstleistungen anzubieten. Viele Arten von Daten, die auf mobilen Endgeräten gespeichert sind oder von diesem Gerät erstellt werden, sind personenbezogene Daten und unterliegen damit den datenschutzrechtlichen Regelungen.

Die Rundfunkanstalt ist datenschutzrechtlich für die Verarbeitung der Daten im Zusammenhang mit der Nutzung einer von ihr angebotenen App verantwortlich. Die Verarbeitung von Nutzerdaten durch die App-Store-Betreiber bei der Anmeldung zum Store und dem Herunterladen einer App liegt hingegen außerhalb ihrer Verantwortung.

Im April 2016 hat der **rbb** für seine neu geschaffene digitale Informationsmarke rbb|24 eine mobile App für die Betriebssysteme iOS und Android veröffentlicht. Sie entspricht den beschriebenen rechtlichen Rahmenbedingungen.

Bei ihrer Entwicklung wurde auf eine datenschutzgerechte Gestaltung („privacy by design“) sowie auf datenschutzfreundliche Voreinstellungen („privacy by default“) geachtet.

Bei der Installation der App werden zur Erbringung des Dienstes bestimmte Berechtigungen auf das Endgerät beim Nutzer eingefordert. Die teilweise recht global formulierten Berechtigungen (z. B. der Telefonstatus) erscheinen auf den ersten Blick als zu weitgehend, sind aber für einzelne Funktionalitäten der App notwendig (im genannten Beispiel muss der Telefonstatus von der App überwacht werden, damit Audios/Videos nicht während eines Telefonates weiterlaufen). Zur Aufklärung über die Notwendigkeit der Berechtigungen wurde in Abstimmung mit mir ein entsprechender Hinweis an die Nutzer entworfen. Über Art, Umfang und Zweck des Datenhandling und das pseudonymisiertes Tracking in der App (mit Möglichkeit zum Opt-Out) wird in der App- internen Datenschutzerklärung aufgeklärt. Der Zugriff auf aktuelle Daten über die App erfolgt über die **rbb**- Webserver.

Bis zum Herbst wird zur Einhaltung der Datensicherheit sowohl beim Versand als auch beim Empfang von Daten zwischen Nutzer und **rbb** die Kommunikationsverbindung mit dem Backend durch eine Transportverschlüsselung abgesichert sein.

6. Datenschutz bei Embedding/Social Media Plugins/iFrames

Embedding bedeutet das Einbinden fremder Inhalte auf der eigenen Webseite. Eingebettet werden z. B. Fotos, Audio- und Videofiles, Textnachrichten sowie Social Media Plugins der großen, zumeist US-amerikanischen Anbieter wie Youtube, Twitter und Facebook. Die Social Plugins erleichtern das Teilen von Inhalten auf den sozialen Plattformen. Auch der **rbb** nutzt diese Technik. Problematisch daran ist, dass dabei praktisch eine eigenständige Internetseite in die eigene Website eingebettet wird. Sobald der Nutzer eine Seite der Rundfunkanstalten mit eingebetteten

Inhalten aufruft, wird regelmäßig die IP-Adresse der Nutzer – ohne Vorwarnung, ohne Wissen und möglicherweise gegen seinen Willen - an die Anbieter dieser Inhalte übertragen, ohne dass der Nutzer dieses Angebot angeklickt hat. Durch den Einsatz von Cookies erfassen die Anbieter der eingebetteten Inhalte zudem das individuelle Surfverhalten der Nutzer. Für ein solches User Tracking ist es noch nicht einmal erforderlich, dass der Nutzer beim jeweiligen sozialen Netzwerk eingeloggt oder dort Mitglied ist.

Das Tracking des Nutzungsverhaltens über eingebettete Inhalte ohne Wissen und Wollen der Nutzer ist rechtswidrig. Für ein rechtskonformes Vorgehen habe ich zusammen mit der Online-Koordination folgende Empfehlung erarbeitet: Die Verwendung der Inhalte muss gegen die datenschutzrechtlichen Risiken im Einzelfall abgewogen werden. Dabei ist die jeweilige Datenschutzpolicy des Drittanbieters zu berücksichtigen. Eine wirkliche Kontrolle, was die Einbettung tatsächlich auslöst, gibt es allerdings nicht. Empfohlen wird deshalb in jedem Fall – ggf. in Ergänzung zu etwaigen datenschutzfreundlichen Voreinstellungen - die Nutzung der von heise.de entwickelten sog. Zwei-Klick-Lösung. Bei dieser Lösung beginnen die eingebetteten Seiten erst nach der Aktivierung einer Zwischenschaltfläche durch den Nutzer mit der Datenübertragung. Der Nutzer wird, sobald er über die Schaltfläche mit dem Mauszeiger fährt, über die Datenweitergabe informiert. Zur besseren Handhabung haben wir inzwischen eine modifizierte Zwei-Klick-Lösung entwickelt. Dabei gibt es für den Nutzer die Möglichkeit, pro Session der Datenübermittlung bei embedding generell zuzustimmen, so dass er die Zwischenschaltfläche nur einmal wegklicken muß.

7. Scribble live

Seit 2013 nutzt der **rbb** wie alle anderen ARD-Anstalten das Social-Media-Modul „Scribble live“. Dieses Modul eignet sich unter anderem für den Einsatz als Liveticker oder Chatmodul. Während des Livetickers oder Chats können sich Nutzer über verschiedene Wege beteiligen – z. B. über Facebook und Twitter – oder direkt kommentieren. Bilder, Links und Socialmedia-Einträge können eingebunden werden. Das Tool kann moderiert und unmoderiert eingesetzt werden.

In dem Vertrag mit Scribble live, den der SWR federführend für die gesamte ARD abgeschlossen hat, wurde die Einhaltung der deutschen Datenschutzbestimmungen ausdrücklich vereinbart. Dieses umfasst auch die Zusicherung von Scribble live, dass die Daten der Nutzer bei Verwendung des Tools nicht unmittelbar und ohne Vorwarnung an die Betreiber der Drittplattformen übermittelt werden. Dazu wurde eigens für die ARD eine technische Lösung entwickelt.

Im Mai 2016 hat Scribble live ein neues Backend-Interface eingeführt. Im Zuge dieser Umstellung ist es zu einem Problem mit der für die ARD programmierten Lösung gekommen. Beim Aufruf von ARD-Angeboten mit Scribble live-Einbindung wurden die Nutzer ohne vorherige Abfrage auch mit den Drittplattformen wie Facebook und Twitter verbunden. Entsprechende Beschwerden von Nutzern haben auch mich erreicht. Durch die Einspielung eines Software-Updates konnte die Problematik durch Scribble live nach einigen Tagen behoben werden.

8. Social Media Tool Swat.io

Federführend für die gesamte ARD hat der SWR Ende 2015 das Social Media Tool Swat.io des Wiener Unternehmens „die socialisten" angeschafft. Dieser browserbasierte Dienst im Internet (Software as a Service) ermöglicht einen Zugriff auf sämtliche Social Media-Plattformen, auf denen die Rundfunkanstalten ihre Inhalte verbreiten (z. B. Facebook, Instagram, Twitter und YouTube), und bietet u. a. die Möglichkeit die Erstellung von Posts auf den Plattformen zu planen, Team-Informationen bei neuen Kommentaren und Nachrichten über alle erfassten Social-Media-Kanäle hinweg zu erstellen und über eine Ticket-Verwaltung die Aktivitäten der Mitarbeiterinnen und Mitarbeiter der Rundfunkanstalten auf den Plattformen zu koordinieren. Außerdem sind verschiedene statistische Auswertungen der Entwicklung der Community möglich. Das Hosting der technischen Infrastruktur wird von einem ebenfalls in Wien ansässigen Vertragspartner der „socialisten" bereitgestellt. Zusätzlich werden bestimmte Daten mittels Amazon Web Services in einem von Amazon in Frankfurt am Main betriebenen Datacenter gespeichert.

Nachdem mir die **rbb**-Online-Koordination dieses Tool mit seinen Möglichkeiten demonstriert hat und ich in einer vom SWR organisierten Telefonschaltkonferenz mit dem Anbieter meine noch offenen Fragen klären konnte, habe ich der Einführung dieses Tools beim **rbb** zu Anfang 2016 zugestimmt. Entscheidend war für mich dabei, dass auf mein Betreiben ARD-weit die Möglichkeit der Auswertung der Aktivitäten einzelner Mitarbeiterinnen und Mitarbeiter der Rundfunkanstalten technisch ausgeschlossen wurde. Darüber hinaus habe ich mit der Online-Koordination verabredet, dass der **rbb** auch die bestehende Auswertungsmöglichkeit der Aktivitäten einzelner Fans nicht benutzen wird. Darauf wurden alle Anwender des Systems bei der Einführung des Systems verpflichtet. Außerdem hat die Online-Koordination auf mein Anraten zusätzlich zu dem vom SWR für die ARD geschlossenen Vertrag für den **rbb** die im Berliner Datenschutzgesetz vorgeschriebene Vereinbarung über Auftragsdatenverarbeitung mit dem Anbieter abgeschlossen, in der die Festlegungen zu Datenschutz und Datensicherheit ergänzt und konkretisiert sind.

V. Datenschutz bei der Rundfunkteilnehmerdatenverarbeitung

1. Datenschutz beim Zentralen Beitragsservice in Köln

1.1 Allgemeines

Für den Einzug der Rundfunkbeiträge betreiben die Landesrundfunkastalten auf der Grundlage von § 10 Abs. 7 Rundfunkbeitragsstaatsvertrag im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft den Zentralen Beitragsservice „ARD ZDF Deutschlandradio Beitragsservice“ (ZBS) in Köln. Soweit der ZBS für den **rbb** tätig wird gelten die bereichsspezifischen Datenschutzregelungen des Rundfunkbeitragsstaatsvertrages und ergänzend die Regelungen des Berliner Datenschutzgesetzes.
Die Überwachung des Datenschutzes bei der Verarbeitung der Rundfunkteilnehmerdaten obliegt der Beauftragten für den Datenschutz des Landes Berlin im Benehmen mit der Landesbeauftragten für den Datenschutz des Landes Brandenburg (§ 38 Abs. 8 rbb-Staatsvertrag). Als behördliche Datenschutzbeauftragte gemäß § 19 a BerlDSG bin ich für die ordnungsgemäße Datenverarbeitung beim **rbb** und beim ZBS unmittelbar zuständig.

Unbeschadet der Zuständigkeit des nach Landesrecht für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ist beim ZBS gemäß § 11 Abs. 2 Satz 1 RBStV eine behördliche Datenschutzbeauftragte des Beitragsservices zu bestellen. Die behördliche Datenschutzbeauftragte arbeitet zur Gewährleistung des Datenschutzes mit dem/der nach Landesrecht für die jeweilige Rundfunkanstalt zuständigen Datenschutzbeauftragten zusammen und unterrichtet diese/n über Verstöße gegen Datenschutzvorschriften sowie über die dagegen getroffenen Maßnahmen. Im Übrigen gelten die für die behördlichen Datenschutzbeauftragten anwendbaren Bestimmungen des Bundesdatenschutzgesetzes entsprechend. Die behördliche Datenschutzbeauftragte übt diese Aufgabe neben ihrer Tätigkeit als Leiterin der Abteilung Zentrale Aufgaben beim ZBS aus. Seit 1. Juni 2006 wird sie durch eine Vollzeitkraft bei der Wahrnehmung ihrer Datenschutzaufgaben unterstützt.

1.2 Stellung der Datenschutzbeauftragten beim Zentralen Beitragsservice

Die Datenschutzbeauftragte und ihr Mitarbeiter leisten seit Jahren sehr professionelle und kompetente Arbeit, wofür die Datenschutzbeauftragten der Landesrundfunkanstalten ihnen sehr dankbar sind. Es ist im Wesentlichen ihr Verdienst, dass der ZBS aus datenschutzrechtlicher Sicht gut aufgestellt ist und das Vertrauen in der Bevölkerung genießt. Umso ärgerlicher ist es, dass in jüngerer Zeit der Eindruck entstand, einige Fachbereiche im ZBS versuchten, sich über wichtige Hinweise und Empfehlungen der Datenschutzbeauftragten hinwegzusetzen. Ich habe dies gegenüber dem Verwaltungsdirektor kritisiert. Auch meine Kolleginnen und Kollegen in den anderen Landesrundfunkanstalten haben entsprechende Signale gegeben. Die Geschäftsleitung des ZBS wurde inzwischen von den Aufsichtsgremien zu einer Stellungnahme aufgefordert.

1.3 Änderung der Verwaltungsvereinbarung „Beitragseinzug“

Derzeit findet eine Überarbeitung der Verwaltungsvereinbarung „Beitragseinzug“ unter der Federführung der Verwaltungsdirektorin des NDR statt. Aus meiner Sicht

wäre dies eine gute Gelegenheit, die Themen „Datenschutz und Informationssicherheit“ in die Verwaltungsvereinbarung einzubringen, da deren derzeitige Fassung dazu keine Regelungen enthält. Derzeit bin ich noch auf der Suche nach Mitstreitern, um einen entsprechenden Vorschlag einzubringen.

1.4 Auskunftsersuchen und Eingaben

Die Datenschutzbeauftragten der Rundfunkanstalten haben die Bearbeitung und Beantwortung von Anfragen und sonstigem Routineschriftwechsel in Datenschutzangelegenheiten dem ZBS übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter und von individuellen Anfragen mit besonderer datenschutzrechtlicher Bedeutung haben sie sich selbst vorbehalten.
Im Jahr 2015 hat die Datenschutzbeauftragte des ZBS folgend Vorgänge aus dem Sendegebiet des **rbb** für mich bearbeitet:

Ersuchen von Bürgerinnen und Bürgern um Auskunft über zu ihrer Person gespeicherter Daten:	53 (Vorjahr 60)
Fragen bezüglich der Herkunft von Daten (z.B. Adressen) bzw. der Berechtigung zur Datenerhebung:	3 (Vorjahr 4)
Verlangen, gespeicherte personenbezogene Daten Zu löschen, zu sperren oder zu berichtigen:	35 (Vorjahr 48)
Anfragen von Finanzämtern nach Daten (insbesondere Bankverbindungen) von Beitragszahlerinnen und –zahlern :	1 (Vorjahr 0)
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz:	3 (Vorjahr 19)
Anzahl der Vorgänge insgesamt:	**96(Vorjahr 131)**

Ich selbst habe in 2015 folgende Vorgänge bearbeitet:

Ersuchen von Bürgerinnen und Bürgern um Auskunft über zu ihrer Person gespeicherter Daten:	11 (Vorjahr 12)
Fragen bezüglich der Herkunft von Daten (z.B. Adressen). bzw. der Berechtigung zur Datenerhebung:	1 (Vorjahr 0)
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen:	1 (Vorjahr 0)
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz:	2 (Vorjahr 7)
Anzahl der Vorgänge insgesamt:	**15 (Vorjahr 24)**

2. Datenschutz beim rbb-Beitragsservice

Wie berichtet, hat der **rbb** mit Wirkung zum 1. März 2015 die telefonische Beratung im nichtprivaten Bereich (np) auf die wdr mediagroup dialog GmbH, eine 100%ige Tochter des WDR , übertragen.

Aufgrund der konstruktiven Zusammenarbeit mit dem Unternehmen in 2015 wurde für 2016 ein weiterer Vertrag abgeschlossen. In diesen neuen Vertrag flossen die Erfahrungen aus 2015, die die Auftragnehmerin bei der NP-Sachverhaltsklärung sowohl für den **rbb** als auch für den WDR erlangt hatte, ein. Es hatte sich herausgestellt, dass die Sachverhaltsklärung ohne jeglichen Zugriff auf das elektronische System zur Verwaltung der Beitragskonten beim ZBS RUBIN wenig effizient ist.

In Abstimmung mit mir wurde der Auftragnehmerin ein begrenzter Zugriff auf RUBIN eingeräumt. Die Auftragnehmerin hat uns dafür ein schlüssiges Informationssicherheitskonzept vorgelegt.

Die ersten Monate haben gezeigt, dass die Beratung nun wesentlich kompetenter erfolgen kann. Dies ist für den **rbb** mit zusätzlichen Neuanmeldungen verbunden und vermeidet fälschliche Doppelanmeldungen. Außerdem können Auskünfte im Hinblick auf die monatliche Beitragshöhe erteilt werden. Zu den Aktivitäten der wdr-media group für den **rbb** haben den **rbb** bislang keinerlei Beschwerden erreicht.

3. Datenschutzprüfung bei der Creditreform Mainz Albert Naujoks KG

Im Auftrag der Landesrundfunkanstalten bzw. des ZBS als deren gemeinsamen Rechenzentrums führt die Firma Creditreform Mainz Albert & Naujoks KG das Inkasso ausstehender Rundfunkbeitragsforderungen durch. Bleiben Vollstreckungsmaßnahmen der Rundfunkanstalten bei den Beitragspflichtigen erfolglos, versucht die Creditreform in Abstimmung mit den Landesrundfunkanstalten und des ZBS in Köln, die säumigen Schuldner doch noch zur Zahlung zu bewegen.

Der Datenschutzbeauftragte des SWR, Herr Prof. Herb, führt stellvertretend für die Datenschutzbeauftragten der anderen Landesrundfunkanstalten in unregelmäßigen Abständen Datenschutzkontrollen bei der Creditreform durch. Die letzte Datenschutzkontrolle fand am 1. Juni 2016 statt. Die Prüfung wurde gemeinsam mit dem Leiter der Revision und der IT-Revisorin des ZBS durchgeführt. Im Ergebnis konnte der Creditreform ein weiterhin hohes Datenschutzniveau bei der Bearbeitung der Beitragsangelegenheiten bescheinigt werden. Hervorzuheben ist, dass die strikte Trennung der Clients im Beitragsinkasso vom Internet aufrechterhalten wurde.

D. Datenschutz im Informationsverarbeitungszentrum (IVZ)

Beim **rbb** wird als Gemeinschaftseinrichtung von DW, DRadio, MDR, NDR, RB, rbb, SR und WDR das rechtlich unselbstständige Informationsverarbeitungszentrum (IVZ) betrieben. Dort werden für die beteiligten Anstalten zentral Aufgaben der elektronischen Datenverarbeitung abgewickelt. Seit 2013 hat das IVZ auch einen größeren Standort beim WDR in Köln.

Für die Kontrolle des Datenschutzes und der Datensicherheit sind die Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Als Datenschutzbeauftragte der Sitzanstalt bin ich federführend für das IVZ zuständig. Ich werde regelmäßig vom IVZ und der dortigen Informationssicherheitsbeauftragten in alle datenschutzrechtlich relevante Fragen und Vorgängen einbezogen.

Am 1. Dezember 2015 fand das Jahrestreffen zu Datenschutz und Informationssicherheit im IVZ 2015 statt. In diesem jährlich wiederkehrenden Termin informiert die Geschäftsleitung des IVZ die Datenschutzbeauftragten und Informationssicherheitsbeauftragten der am IVZ beteiligten Rundfunkanstalten über aktuelle Projekte mit datenschutzrechtlicher Relevanz. Außerdem erstattet die Informationssicherheitsbeauftragte einen Bericht zu Informationssicherheitsaspekten.

Themen waren u. a. der Nutzungsstand der ARDBox, eine Studie zum Virtual Data Center, in dem mit OpenStack ein neues Modell einer Virtualisierung der gesamten Speicher/Server-Infrastruktur des IVZ möglich wäre, der Verlauf und die Schwerpunkte der BSI-Zertifizierungs-Audits 2015 und einzelne Sicherheitsvorfälle im IVZ.

Die private Nutzung von iOS-Geräten wurde kontrovers diskutiert. Die Datenschutzbeauftragten und die Informationssicherheitsbeauftragten der Rundfunkanstalten haben das IVZ um eine sofortige Einstellung der Privatnutzung von Bereitschaftsgeräten gebeten.

E. Informationsmaßnahmen

In 2015 habe ich mit dem Leiter OUI Herrn Kruithof, ein Seminar speziell für Führungskräfte zu den Themen „Datenschutz und Informationssicherheit“ entwickelt und an folgenden Terminen durchgeführt: am 8. September und 17. November 2015 und am 2. Mai und 20. Juni 2016.

Ich begrüße es sehr, dass die Teilnahme an dem Seminar für Führungskräfte seit Anfang 2016 verpflichtend ist. Aus meiner Sicht ist es wichtig, dass gerade die Führungskräfte des Hauses ein Bewusstsein für Datenschutz und Informationssicherheit haben, mit gutem Beispiel vorangehen und auch zu diesen Themen auch gegenüber ihren Mitarbeiterinnen und Mitarbeitern auskunftsfähig sind. Die Resonanz auf unsere Veranstaltung bestätigt, dass die Durchführung derartiger Schulungen auch ganz im Sinne der Teilnehmerinnen und Teilnehmer ist. Denn bei der Verarbeitung von Mitarbeiterdaten bestehen auch bei vielen Führungskräften immer wieder gewisse Unsicherheiten.

Am 20. August 2015 habe ich gemeinsam mit Herrn Kruithof das jährliche Datenschutzseminar für die neuen Auszubildenden beim **rbb** durchgeführt.

Unterweisungen zum Datenschutz bei SAP habe ich bzw. mein Stellvertreter gemeinsam mit einer Kollegin aus der OUI am 9. September und 4. November 2015, 19. Januar, 11. Februar, 5. April, 7. Juni 2016 durchgeführt.

Am 15. Oktober 2015 habe ich eine Datenschutzunterweisung für die künftigen Nutzer des neuen Dispositionssystems MIRAAN bei Inforadio durchgeführt.

Nach wie vor setze ich mich dafür ein, dass es im **rbb** neben Präsenzschulungen zukünftig Online-Schulungen zu den Themen Datenschutz und Informationssicherheit gibt. Da ich ein solches Angebot technisch und inhaltlich nicht allein stemmen kann, bin ich mit der für Schulungen zuständigen Personalabteilung im Gespräch. Auch die Personalabteilung ist an eLearning-Angeboten z. B. im Bereich Arbeits-

schutz interessiert und hat ein erstes Gespräch mit einem Anbieter geführt. An diesem Gespräch hat auch mein Stellvertreter teilgenommen.

F. 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.
Im Berichtszeitraum fanden Sitzungen am 12. und 13. März 2015 beim SWR in Karlsruhe, am 24./25. September 2015 bei Arte G.E.I.E. in Straßburg und am 14./15. April 2016 beim **rbb** in Berlin statt.

Auf der Sitzung in Karlsruhe haben wir uns u. a. mit Fragen rund um den Minderjährigendatenschutz in den Online-Angeboten der Rundfunkanstalten, mit Datenschutz bei HbbTV und mit vielen Einzelfragen zum Thema Datenschutz beim Rundfunkbeitragseinzug beschäftigt. Außerdem hatten wir in den Räumlichkeiten des Bundesverfassungsgerichts die Gelegenheit zu einem Gespräch mit dem für Datenschutz zuständigen Referenten des Verfassungsrichters Prof. Masing, Herrn Dr. Hammer, zu aktuellen datenschutzrechtlichen Fragen – insbesondere im Medienbereich.

In Straßburg haben wir Frau Rebecca Thery, die Datenschutzbeauftragte und stellvertretende Justitiarin von ARTE G.E.I.E kennengelernt. Sie stellte uns unter anderem den ARTE Club – ein personalisiertes Webangebot – vor. Dabei müssen weder ein Benutzerkonto angelegt, noch die Speicherung von Cookies zugelassen werden. Der User allein entscheidet, welche Informationen er ARTE überlassen möchte. Wahlweise kann der User auch ein Benutzerkonto erstellen. Dies geschieht im SSO-Verfahren („Single-Sign-On"). Ich halte dieses Konzept für sehr interessant und würde dem **rbb** ggf. empfehlen, zumindest einige Elemente davon zu übernehmen. Des Weiteren haben wir uns auch mit Fragen zur Datenschutzgesetzgebung und –politik und mit zahlreichen ARD-internen Themen wie einer neuen Vergabesoftware und der ARD-Box beschäftigt.

In Berlin standen Umsetzungsfragen im Zusammenhang mit der DS-GVO und Datenschutzfragen beim Beitragsservice in Köln im Fokus.

II. Vertretung des AK DSB in der Europäischen Datenschutzgruppe nach Art. 29 der EG-Datenschutzrichtlinie

Art. 29 Abs. 2 EU-Datenschutzrichtlinie sieht die Einsetzung einer Europäischen Datenschutzgruppe vor, die aus Vertretern der einzelnen Mitgliedstaaten der EU besteht. Diese Gruppe berät die EU-Kommission und trägt zur einheitlichen Anwendung der Datenschutzrichtlinie in den EU-Staaten bei. Seit Ende 2001 ist eine Vertreterin bzw. ein Vertreter des AK DSB an der Gruppe beteiligt. Dies ist nach wie vor der Datenschutzbeauftragte des Norddeutschen Rundfunks Herr Brendel. Dadurch ist eine regelmäßige Information der Landesrundfunkanstalten über die sich abzeichnende Entwicklung und Meinungsbildung im Bereich des Datenschutzes auf europäischer Ebene sichergestellt.

III. Arbeitskreis Medien der Datenschutzbeauftragten von Bund und Ländern

Im Arbeitskreis Medien diskutieren die Datenschutzbeauftragten von Bund und Ländern unter dem Vorsitz der Berliner Beauftragten für Datenschutz aktuelle und strategische Fragen des Datenschutzes aus den Bereichen des Telekommunikations-, Multimedia- und Rundfunkrecht. An einem Teil der Sitzung nimmt regelmäßig ein Vertreter des AK DSB teil. Der AK DSB hat mich mit dieser Aufgabe betraut.

Im Berichtszeitraum habe ich den AK DSB auf der Sitzung des AK Medien am 23. September 2015 vertreten. Dabei ging es um Datenschutz um HbbTV /SmartTV und um die Evaluations des Rundfunkbeitragsstaatsvertrages. Auf der Sitzung am 2. März 2016 hat in meiner Vertretung meine Kollegin vom SR Sonnia Wüst den AK DSB vertreten.

IV. Arbeitskreis Informationssicherheitsgremium

Der Datenschutzbeauftragte des SWR, Herr Prof. Herb, hat im SWR auch die Funktion des Informationssicherheitsbeauftragten inne. In dieser Funktion ist er ordentliches Mitglied im Informationssicherheitsgremium und hat die Vertretung des AK DSB in diesem Gremium übernommen. Über die wesentlichen Ergebnisse aus den Sitzungen wird dem AK DSB regelmäßig berichtet.

V. Teilnahme an Fortbildungen und Veranstaltungen

Am 5. November 2015 habe ich eine Veranstaltung der Stiftung Datenschutz zur DS-GVO in Berlin besucht.

Am 28. April 2016 habe ich an einem Workshop des Instituts für Europäisches Medienrecht EMR für Anbieter von Mediendiensten, Hersteller von Smart-TV-Geräten und das interessierte Fachpublikum zum Thema „Smart Devices, Personal TV und interaktive Dienste: Was bringt die neue Datenschutz-Grundverordnung der EU?“ teilgenommen. Dabei zeigte sich, dass hinsichtlich der Umsetzung der DS-GVO in die Praxis noch Klärungsbedarf besteht. Smart-TV ist in der Verordnung nicht explizit erwähnt, aber die dort aufgestellten Regeln gelten auch für das moderne Fernsehen. Zugleich wurde auch die Anwendung der bestehenden Regeln kontrovers diskutiert.

Am 11. Mai 2016 habe ich am 20. Berliner Kolloquium der Daimler Benz Stiftung zum Thema „Der Datenmensch - Freiheit und Selbstbestimmung in der digitalen Welt“ teilgenommen. Dabei ging es vor allem um die Fragen, ob das datenschutzrechtlichen Institut der informierten Einwilligung, der Zweckbindungsgrundsatz und das Gebot der Datensparsamkeit im Zeitalter von Big Data überhaupt noch aufrechterhalten werden können. Interessant war vor allem der Grundsatz-Vortrag von Herrn Prof. Dr. Johannes Masing, Richter am Bundesverfassungsgericht.

Am 15. Juni 2016 habe ich am **rbb** -internen Fachseminar „Compliance“ der Compliance-Beauftragten des **rbb** Frau Dr. Kerstin Skiba und dem Mitarbeiter der Revision, Herrn Axel Kauffmann teilgenommen.

Am 13. Und 14. Juni 2016 habe ich am COMPUTAS -Datenschutzkongress in Berlin teilgenommen und dabei einen guten Überblick über die aktuellen Datenschutzthemen und ihre Diskussionsstände erhalten.

Berlin, 10. August 2016
gez. Anke Naujock

Anlage

Dienstanweisung für Wartungstätigkeiten und Auftragsdatenverarbeitung