12. Tätigkeitsbericht

der Beauftragten für den Datenschutz

des

Rundfunk Berlin-Brandenburg

Berichtszeitraum:

01. April 2014 bis 31. März 2015

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

Inhaltsverzeichnis

Vorbemerkung

In der Zeit von Ende April 2013 bis Anfang Mai 2014 konnte ich meinen Dienst im **rbb** krankheitsbedingt nicht ausüben. Während dieser Zeit hat mich der damalige stellvertretende behördliche Datenschutzbeauftragte, Herr Dr. Hans Bismark, vertreten und dem Rundfunkrat auch die letzten beiden Tätigkeitsberichte vorgelegt. Herr Dr. Bismark hielt während dieser Zeit nicht nur einen engen Kontakt zu mir und stimmte sich mit mir - soweit dies möglich war - inhaltlich ab, sondern kümmerte sich mit großer Anteilnahme um mein seelisches Wohlergehen. Dafür möchte ich Herrn Dr. Bismark an dieser Stelle noch einmal ausdrücklich danken. Inzwischen befindet er sich im wohlverdienten Ruhestand. Zu seinem Nachfolger hat die Intendantin mit Wirkung zum 1. April 2014 den Mitarbeiter der Revision, Herrn Axel Kauffmann, ernannt.

Als ich im Frühjahr 2014 meine Tätigkeit im **rbb** wieder aufnahm, nahm ich einen frischen Wind wahr: Nachdem meine Bemühungen, dem Thema Informationssicherheit mehr Aufmerksamkeit zu verschaffen, noch in den Vorjahren eher zurückhaltend aufgenommen worden waren, hatte sich inzwischen neben dem Informationssicherheitsbeauftragten, Herrn Gerry Wolff, auch der Leiter des Bereichs Organisation und IT (OUI), Herr Thomas Kruithof, persönlich des Themas angenommen. Der Informationssicherheit wird zu meiner großen Freude jetzt ein weitaus höherer Stellenwert beigemessen. Im Berichtszeitraum haben Herr Kruithof und ich in Informationssicherheitsthemen sehr eng zusammengearbeitet und unter anderem gemeinsam eine Schulung zu Datenschutz und Informationssicherheit für die Führungskräfte und andere Zielgruppen im **rbb** konzipiert. Dabei wurden wir dankenswerter Weise von einer Mitarbeiterin der OUI unterstützt, die mit großem Kommunikationstalent dabei half, die im Bewusstsein der Kolleginnen und Kollegen nach wie vor mit vielen Widerständen besetzte Thematik lebensnah und interessant aufzuarbeiten. Außerdem haben wir verschiedene Informationsflyer verteilt und diverse Artikel im Intranet veröffentlicht. Der Angriff von Cyber-Kriminellen in der Nacht vom 8. /9. April 2015 auf den französischen Fernsehsender TV5 hat ein Übriges dazu getan, dass sich inzwischen auch wirklich jeder/jede hier im Sender Ge-

danken zur Informationssicherheit machen dürfte. Schließlich wurde unter der Leitung des Informationssicherheitsbeauftragten ein Informationssicherheitskreis aus Vertretern aller Direktionen gegründet, dem u. a. auch der Personalrat und die Datenschutzbeauftragte angehören. Das ambitionierte Ziel eines funktionierenden Informationssicherheitsmanagement mit klar definierten Rollen, Aufgaben und Verantwortlichkeiten hat erste gute Ansätze erfahren. Nun muss es weiter mit Leben gefüllt werden. Auch die Schulungs- und Sensibilisierungsmaßnahmen müssen weiter fortgesetzt werden. Dazu werde ich selbstverständlich meinen Teil beitragen. Allerdings ist absehbar, dass ich dafür projektbezogen auf personelle Unterstützung angewiesen sein werde.

Einen weiteren Schwerpunkt bildeten im Berichtszeitraum Fragen des Datenschutzes im Programmbereich, insbesondere beim Thema HbbTV. Gemeinsam mit meinem Kollegen vom Mitteldeutschen Rundfunk, Herrn Stephan Schwarze, haben wir mit dem ARD-Play-Out-Center (POC) in Potsdam ein datenschutzkonformes Verfahren entwickelt, mit dem die ARD nun bundesweit Vorreiter ist.

Außerdem war ich mit zahlreichen Einzelfragen zum Datenschutz im **rbb** befasst.

Herr Kauffmann hat sich von Anfang an mit großem Engagement in das für ihn neue Fachgebiet eingearbeitet. Bei großen Projekten beziehe ich ihn von vornherein mit ein. Die Zusammenarbeit mit ihm macht mir große Freude. Auch meiner Kollegin im Sekretariat, Frau Ruthild Just, die inzwischen in den Ruhestand gegangen ist, und ihrer Nachfolgerin, Frau Anja Hubert, danke ich für ihre Unterstützung. Die Zusammenarbeit mit der Geschäftsleitung und dem Personalrat war auch im Berichtszeitraum wieder sehr konstruktiv und angenehm.

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

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. November 2011 hat mich der Rundfunkrat gemäß § 38 Abs. 1 **rbb**-Staatsvertrag auf Vorschlag der Intendantin für eine weitere Amtszeit von vier Jahren 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. Auch die Amtszeit des stellvertretenden behördlichen Datenschutzbeauftragten, Herrn Dr. Bismark, war entsprechend verlängert worden. Während meiner krankheitsbedingten Abwesenheit von Ende April 2013 bis Anfang Mai 2014 hat Herr Dr. Bismark sämtliche datenschutzrechtlichen Vorgänge im **rbb** selbstständig bearbeitet.

Nach Ausscheiden von Herrn Dr. Bismark in den Ruhestand hat die Intendantin mit Wirkung zum 1. April 2014 den Mitarbeiter der Revision, Herrn Axel Kauffmann, zum stellvertretenden behördlichen Datenschutzbeauftragten bestellt. Herr Kauffmann vertritt mich in Abwesenheitsfällen. Außerdem haben wir verabredet, dass ich datenschutzrechtliche Anfragen und Beschwerden mit möglichen Berührungspunkten zu meiner Tätigkeit im Justitiariat (z. B. im Arbeitsrecht) von vornherein an ihn zur Bearbeitung abgebe, um auf diese Weise eine etwaige Interessenskollision bzw. den Anschein einer solchen zu vermeiden.

Seit Beginn des Wirtschaftsjahres 2015 hat die Datenschutzbeauftragte eine eigene Kostenstelle für den Datenschutz als Unterkostenstelle zu den Gremien. Diese Veränderung entspricht einer langjährigen Forderung von mir und unterstreicht die unabhängige Stellung der Rundfunkdatenschutzbeauftragten.

Zum Beginn des Jahres 2015 habe ich meine Aktenführung auf das elektronische Dokumentenverarbeitungssystem WinRa umgestellt. Ich nutze das System gemein-

sam mit dem Justitiariat und der Beteiligungsverwaltung. Durch das Berechtigungskonzept ist gewährleistet, dass keine unbefugten Nutzer des Systems auf die Datenschutz-Akten zugreifen können.

Für die Datensicherheit im **rbb** ist der Systemverantwortliche für Informationssicherheit, Herr Gerry Wolff, verantwortlich.

Die datenschutzrechtliche Kontrolle durch den Berliner Landesdatenschutzbeauftragten in Abstimmung mit der Brandenburgischen Datenschutzbeauftragten gemäß § 38 Abs. 8 **rbb**-Staatsvertrag beschränkte sich auch im Berichtszeitraum im Wesentlichen wieder auf die Einhaltung des Datenschutzes beim Rundfunkbeitragseinzug.

B. Entwicklung des Datenschutzrechts

I. Europa

1. Neue Datenschutz-Grundverordnung

In den Vorjahren hatte ich über die Bestrebungen auf Europäischer Ebene zur Novellierung des EU-Datenschutzrechts berichtet. Die geplante Datenschutz-Grundverordnung betrifft auch den Datenschutz im Medienbereich, so dass die Rundfunkanstalten unmittelbar von der Neuregelung betroffen sein werden. Die EU-Mitgliedsstaaten haben Mitte Juni 2015 eine gemeinsame Position beschlossen. Auf dieser Basis soll nun mit dem Europäischen Parlament verhandelt werden. Eine Einigung soll nach dem Willen aller Seiten bis Ende des Jahres im Rahmen von Trilogverhandlungen in der ersten Lesung erreicht werden.

Im Hinblick auf die für den öffentlich-rechtlichen Rundfunk besonders wichtige Regelung zur „journalistischen Ausnahme“ (Art. 80) sind die Vorschläge der Mitgliedstaaten weitgehend zu begrüßen. Die Anliegen des öffentlich-rechtlichen Rundfunks

werden weitgehend berücksichtigt. Laut aktuellem Zeitplan sollen die entsprechenden Artikel im September und November 2015 im Trilog verhandelt werden.

2. Urteile

Entscheidung des Europäischen Gerichtshofs für Menschenrechte zur Vorratsdatenspeicherung

Die EU-Richtlinie zur Vorratsdatenspeicherung, die eine anlasslose Vorratsspeicherung von Verkehrs- und Bestandsdaten für mindestens 6 Monate vorsah, verstieß gegen europäisches Recht und ist ungültig. Das hat der Europäische Gerichtshof (EuGH) mit Urteil vom 8. April 2014 entschieden. Das Gericht erteilte der undifferenzierten und automatischen Erfassung von Verkehrsdaten in der Telekommunikation eine Absage. Zwar werde der Wesensgehalt der Achtung der Privatsphäre (Art. 7 der Europäischen Grundrechtscharta), des Schutzes personenbezogener Daten (Art. 8) und der Meinungsfreiheit (Art. 11) durch die Vorratsdatenspeicherung nach Ansicht des EuGH nicht angetastet, solange sie den Inhalt der elektronischen Kommunikation nicht zur Kenntnis gibt, die Grundsätze des Datenschutzes und der Datensicherheit eingehalten sowie die Inhalte von Nachrichten der mit Hilfe eines elektronischen Kommunikationsnetzes abgerufenen Informationen nicht offen gelegt werden. Die Vorratsdatenspeicherung, wie sie der EuGH zu beurteilen hatte, sei allerdings ein Eingriff in die genannten Grundrechte von großem Ausmaß, der als besonders schwerwiegend anzusehen sei. Dieser Eingriff müsse, um rechtmäßig zu sein, nicht nur geeignet sein, die verfolgte Zielsetzung zu erreichen. Er müsse auch erforderlich und verhältnismäßig sein, dürfe also die Grenzen dessen nicht überschreiten, was zur Erreichung des Ziels geeignet und erforderlich sei. Die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, sei zwar von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit und deren Wirksamkeit könne in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen. Diese dem Gemeinwohl dienende Zielsetzung könne die Speicherungsmaßnahme für die Kriminalitätsbekämpfung für sich genommen aber nicht rechtfertigen, soweit die Speicherung auf Vorrat, also anlasslos und ohne jede Differenzierung, vorgenommen wird.

Der EuGH fordert, dass für Personen, deren Kommunikationswege nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen, Ausnahmen vorzusehen seien. Zu den Berufsgeheimnisträgern in diesem Sinne gehören die Journalistinnen und Journalisten.

In Deutschland war die Vorratsdatenspeicherung per Gesetz auf Basis der EU-Richtlinie im Jahr 2007 eingeführt worden. Mit Urteil vom 2. März 2010 hatte das Bundesverfassungsgericht (BVerfG) dieses Gesetz für verfassungswidrig und nichtig erklärt. Zur Begründung hatte das Gericht ausgeführt, dass das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit vorsehe und zudem die Hürden für staatliche Zugriffe auf die Daten zu niedrig seien. Eine Vorratsdatenspeicherung verstößt allerdings auch nach Ansicht des BVerfG nicht generell gegen das Grundgesetz.

Mit dem Wegfall der europarechtlichen Grundlage war auch die Bundesregierung zunächst von ihrem Vorhaben abgerückt, schnell ein neues Gesetz zur Vorratsdatenspeicherung zu erlassen. Allerdings hat das Bundeskabinett vor dem Hintergrund verschiedener terroristischer Anschläge in Europa am 27. Mai 2015 dann dennoch einen neuen Gesetzesentwurf vorgelegt. Die damit verbundenen Eingriffe in die freie Entfaltung der Persönlichkeit, die Kommunikationsgrundrechte und das Fernmeldegeheimnis (Art. 2, 5, 10 GG; Art. 7, 8 und 11 der Grundrechtecharta der Europäischen Union) sollen sich damit nach Ansicht der Bundesregierung in zulässigem Rahmen bewegen. Vorgesehen ist jetzt eine Speicherdauer für Verbindungsdaten für zehn Wochen; Standortdaten sollen vier Wochen gespeichert bleiben.

Nach wie vor bestehen allerdings erhebliche Zweifel daran, dass die vorgesehene Gesetzgebung die verfolgte Zielsetzung der effektiven Bekämpfung der Kriminalität und des Terrorismus tatsächlich fördert. Statistiken belegen dies jedenfalls bis heute nicht. Auch im Übrigen ist zweifelhaft, ob das Gesetz den Anforderungen der Rechtsprechung des EuGH und des BVerfG genügt. Insbesondere beim Schutz der Berufsgeheimnisträger muss nachgebessert werden.

Urteil des EuGH zum sog. Recht auf Vergessen

Der Suchmaschinenbetreiber Google kann dazu verpflichtet werden, Verweise auf Webseiten mit sensiblen persönlichen Daten aus seiner Ergebnisliste zu streichen. Das entschied der Europäische Gerichtshof in Luxemburg in einem Urteil vom 13. Mai 2014 (Rs.C-131/12) unter Verweis auf die EU-Datenschutzrichtlinie.

Danach muss Google künftig auf Antrag des Betroffenen veraltete oder irrelevante Informationen löschen.

Nach Ansicht des Gerichts ist der Suchmaschinenbetreiber für die Verarbeitung der Daten verantwortlich. Ein Betroffener könne sich mit der Bitte um Änderung der Suchergebnisse direkt an Google wenden. Dies gelte, wenn die Person nachweise, dass sich Links auf veraltete oder irrelevante Informationen bezögen.

Mit der Eingabe eines Namens bei einer Internet-Suchmaschine könnten sich die Nutzer ein umfassendes Bild von dieser Person machen. Die Suchergebnisse seien nichts anderes als das Ergebnis einer Verarbeitung personenbezogener Daten. Das EU-Recht verlange hier einen Ausgleich zwischen den Interessen der Nutzer und denen der betroffenen Personen.

Geklagt hatte ein Spanier. Er wehrte sich dagegen, dass Google bei der Eingabe seines Namens noch heute einen Artikel über die Zwangsversteigerung seines Hauses vor 15 Jahren anzeigt. Die amtliche Bekanntmachung über die Pfändung wurde 1998 in einer Zeitung und im Internet veröffentlicht. Der Kläger argumentierte, dass die Pfändung seit Jahren vollständig erledigt sei und deshalb keine Erwähnung mehr verdiene.

Das Urteil des EuGH ist für die Rundfunkanstalten sehr hilfreich. Denn das Gericht konstatiert in den Entscheidungsgründen, dass aufgrund des datenschutzrechtlichen Medienprivilegs die Medien selbst zur Löschung nicht verpflichtet sind. Dieses Privileg stehe – so das Gericht – den Suchmaschinenbetreibern nicht zu.

Kurz nach dem Erlass des Urteils hat Google einen sog. Löschbeirat einberufen, damit dieser Regeln und Empfehlungen zum Vorgehen bei komplizierten Löschan-

trägen ausarbeitet. Das Gremium, dem auch die frühere Bundesjustizministerin Frau Dr. Sabine Leutheusser-Schnarrenberger (FDP) angehört, konsultierte dazu in zahlreichen europäischen Ländern Sachverständige und diskutiert auch mit der Öffentlichkeit die Folgen des Urteils.

Der Löschbeirat hat Google empfohlen, mehr Anträge zum Recht auf Vergessen als bislang zu bewilligen. Uneinig sind sich die Experten offenbar über die Reichweite des Löschungsanspruchs. Mehrheitlich plädieren sie dafür, dass bei einem Anspruch auf das Löschen von Links nur die Links auf EU-Domains gelöscht werden, wie es seit dem Luxemburger Gerichtsurteil schon Praxis bei Google ist. Demgegenüber fordert Frau Dr. Leutheusser-Schnarrenberger eine globale Löschung für alle Domains. Im Streit über ein weltweites Recht auf Vergessen(werden) im Internet stellt sich Google nun gegen eine Anordnung aus Frankreich. Google erklärte, die Pariser Datenschutz-Aufsicht sei bei der Löschung von Suchergebnissen nicht global zuständig. Der weitere Fortgang dieser Angelegenheit bleibt spannend.

II. Bund

1. Gesetzentwurf zur zivilrechtlichen Durchsetzung datenschutzrechtlicher Vorschriften (Änderung UKlaG, UWG und BGB)

Im Februar 2015 hat die Bundesregierung den Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts vorgelegt. Dieses sieht explizit ein Verbandsklagerecht bei Datenschutzverstößen vor und soll den Verbraucherschutzverbänden die Verfolgung von Datenschutzverstößen ermöglichen. Das Gesetz befindet sich derzeit in der parlamentarischen Beratung.

Die Datenschutzbeauftragten sehen 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 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.

2. Urteile

Urteil des BGH zum Anspruch auf Herausgabe von Nutzerdaten bei Persönlichkeitsrechtsverletzungen

Nach einem Urteil des BGH vom 1. Juli 2014 – VI ZR 345/13 - ist der Betreiber eines Internetportals aufgrund fehlender gesetzlicher Ermächtigungsgrundlage grundsätzlich nicht befugt, personenbezogene Daten eines Nutzers ohne dessen Einwilligung zur Erfüllung eines Auskunftsanspruchs wegen einer Persönlichkeitsrechtsverletzung an den Betroffenen zu übermitteln.

Das Ergebnis einer anonymen Internetnutzung entspricht dem Grundgedanken des Telemediengesetzes (TMG), wonach personenbezogene Daten, die für die Bereitstellung der Telemediendienste erhoben worden sind, grundsätzlich nicht für andere Zwecke verwendet werden dürfen. Die Verwendung von Bestands- und Nutzungsdaten zu Zwecken der Auskunftserteilung ist allein der Strafverfolgung, der Gefahrenabwehr durch die Polizei, der Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes (BND) oder des Militärischen Abschirmdienstes (MAD) oder des Bundeskriminalamtes oder zur Durchsetzung der Rechte am geistigen Eigentum nach § 14 Abs. 2 TMG vorbehalten.

Für den in seinem allgemeinen Persönlichkeitsrecht Verletzten bleibt ein Unterlassungsanspruch gegen den Diensteanbieter. Darüber hinaus besteht die Möglichkeit, im Rahmen eines Strafverfahrens Auskunft über die Identität des Nutzers zu erhalten.

Urteil des BGH zur Speicherung der IP-Adresse bei Telefkommunikations-dienstleistern

Eine auf sieben Tage beschränkte Speicherung von IP-Adressen durch Telekommunikationsdienstleister ist zur Abwehr von Störungen der Telekommunikationsanlage zulässig (§ 96 Abs. 1 S. 2 i.V.m. § 100 Abs. 1 Telekommunikationsgesetz (TKG). Das hat der BGH mit Urteil vom 3. Juli 2014 (III ZR 391/13) entschieden. Die Erwägungen des EuGH in dessen Urteil zur Ungültigkeit der Richtlinie über die Vorratsdatenspeicherung von Daten (s. S. 11 ff.) sind nach Ansicht des BGH auf die siebentätige Speicherung von IP-Adressen zu den in § 100 TKG bestimmten Zwecken nicht übertragbar. Die Speicherung der dynamischen IP-Adresse für sieben Tage sei derzeit mangels technischer Alternativen aus Sicherheitsgründen erforderlich und nach § 100 TKG auch zulässig. Im Übrigen weist der BGH darauf hin, dass die Speicherung nicht für Zwecke der Strafverfolgungsbehörden, sondern im Interesse des Netzbetreibers liegt. Ein Zugriff von Polizei oder Staatsanwaltschaft auf die gespeicherten Daten ist in dieser Rechtsgrundlage nicht vorgesehen.

Urteil des Bundesgerichtshofs zur Vertraulichkeit von privaten E-Mails contra Presse- und Meinungsfreiheit

In seinem Urteil vom 30. September 2014 (VI ZR 490/12) hat der Bundesgerichtshof (BGH) wichtige grundsätzliche Aussagen zum Schutz von privaten E-Mails und der Reichweite der Presse- und Meinungsfreiheit getroffen, die vor allem für den investigativen Journalismus von Bedeutung sein dürften:

1. Das allgemeine Persönlichkeitsrecht in der Ausprägung der Vertraulichkeitssphäre und des Rechts auf informationelle Selbstbestimmung schützt das Interesse des Kommunikationsteilnehmers daran, dass der Inhalt privater E-Mails nicht an die Öffentlichkeit gelangt.
2. Die Veröffentlichung rechtswidrig beschaffter oder erlangter Informationen ist vom Schutz der Meinungsfreiheit umfasst.
3. Werden rechtswidrig erlangte Informationen zum Zwecke der Berichterstattung verwertet, kommt es bei der Abwägung des von den Medien verfolgten Informationsinteresses der Öffentlichkeit und ihres Rechts auf Meinungsfreiheit mit dem Interesse des Betroffenen am Schutz seiner Persönlichkeit maßgeblich auf den Zweck der beanstandeten Äußerung und auf das Mittel an, mit dem der Zweck verfolgt wird.

Klagegegenstand war die Veröffentlichung des Inhalts von privaten Mails des früheren Finanz- und späteren Innenministers von Brandenburg. Die Mails befanden sich auf dessen privatem Laptop, der ihm abhandengekommen war. Die Mails waren verschiedenen Medien zugespielt worden, die den Inhalt veröffentlichten. Aus der E-Mailkorrespondenz mit einer Mitarbeiterin ging hervor, dass der Minister mit dieser eine außereheliche Beziehung unterhalten hatte, aus der eine Tochter hervorgegangen war. Bis auf geringfügige Zahlungen hatte er für diese keinen Unterhalt geleistet. Die Mitarbeiterin hatte über einen längeren Zeitraum Leistungen nach dem Unterhaltsvorschussgesetz erhalten. Den Vater hatte sie den zuständigen Behörden nicht genannt. Es bestand der Verdacht auf Sozialbetrug gegenüber der Mitarbeiterin.

Der BGH wies den vorbeugenden Unterlassungsanspruch des Klägers gegen die Veröffentlichung der Mails ab. Sein Interesse am Schutz seiner Persönlichkeit hätte gegenüber dem Recht der Beklagten auf Meinungs- und Medienfreiheit zurückzutreten. Bei der Abwägung fiel ins Gewicht, dass nicht die Publizierenden selbst sich die Informationen widerrechtlich verschafft hatten, wenngleich ihnen die Rechtswidrigkeit der Informationsbeschaffung nicht verborgen geblieben war. Die Informationen, deren Verbreitung der Kläger mit seinem vorbeugenden Unterlassungsanspruch habe verhindern wollen, offenbarten, dass er aus Eigeninteresse die wirtschaftliche Verantwortung für sein nichteheliches Kind auf den Steuerzahler abgewälzt hatte. Ein derartiges Verhalten sei für die Beurteilung der persönlichen Eignung des Klägers als Finanz- und Innenminister und Landtagsabgeordneter von maßgeblicher Bedeutung. Der Kläger gehöre zu den Personen des politischen Lebens, an deren Verhalten unter dem Gesichtspunkt demokratischer Transparenz und Kontrolle ein gesteigertes Informationsinteresse bestehe.

Unterlassungsklage des VZBV in Sachen KiKa-Online-Gewinnspiele

In meinem 9. und 10. Tätigkeitsbericht hatte ich über das Begehren des Verbraucherzentrale Bundesverband e.V. (VZBV) berichtet, die Abfrage von Daten bei Online-Gewinnspielen im KiKa zu unterlassen.

Bei den Gewinnspielen wurden von den Kindern neben der Antwort der Name, das Alter und der Wohnort abgefragt. Nach Ansicht des VZBV stellt dies einen wettbewerbsrechtlich relevanten Verstoß gegen den Grundsatz der Datensparsamkeit dar. Die Kenntnis der E-Mail-Adresse sei für eine Teilnahme am Gewinnspiel ausreichend. Die vom VZBV vor dem Landgericht Leipzig erhobene Klage war ebenso erfolglos wie die Berufung vor dem Oberlandesgericht Dresden. Die Gerichte sahen in den datenschutzrechtlichen Bestimmungen keine Marktverhaltensregelungen, die einen Verstoß gegen wettbewerbsrechtliche Vorschriften begründen könnten. Die Revision wurde nicht zugelassen. Der BGH hat mit Beschluss vom 13.3.2014 (I ZR 78/13) die Nichtzulassungsbeschwerde zurückgewiesen. Begründet wurde dies allein damit, dass dieses Rechtsmittel mangels Erreichen der dafür erforderlichen Beschwer von über 20.000,00 € bereits nicht statthaft ist. Das klageabweisende Urteil des LG Leipzig vom 17.10.2012 ist damit rechtskräftig.

Dessen ungeachtet hat der KiKa-Geschäftsführer entschieden, bei Online-Gewinnspielen künftig lediglich den Vornamen und die E-Mail-Adresse abzufragen.

Vorlage an den EuGH in Sachen „Speicherung von dynamischen IP-Adressen"

Der BGH hat Ende Oktober 2014 dem Gerichtshof der Europäischen Union unter anderem die Frage zur Auslegung der EG-Datenschutz-Richtlinie vorgelegt, ob eine IP-Adresse, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (der Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt (VI ZR 135/13).

Die Klärung dieser Frage ist auch für den **rbb** von unmittelbarer Relevanz. Denn nur für den Fall, dass die dynamische IP-Adresse tatsächlich ein personenbezogenes Datum darstellt, bedarf ihre Verarbeitung einer speziellen Rechtfertigung und muss der Nutzer entsprechend aufgeklärt werden. So wird von einigen wenigen Kritikern moniert, dass beim HbbTV bereits unmittelbar bei Einschalten eines bestimmten Programms (z.B. Das Erste) die IP-Adresse übermittelt wird, um im Hintergrund schon die ARD-Startleiste mit den Zusatzinformationen hochladen zu können, damit bei Drücken des sog. Red Buttons diese Informationen für den Zuschauer sofort verfügbar sind. Auch speichern die meisten Anbieter von Internetangeboten - so auch der **rbb** - zur Gewährleistung der Betriebssicherheit sowie zum Schutz der Applikationen vor Manipulation durch Dritte die entsprechenden Protokolldaten einschließlich IP-Adresse für eine bestimmte Zeit (in der Regel 7 Tage). Hier besteht insofern eine gewisse Rechtsunsicherheit, als es an einer eindeutigen Rechtsgrundlage dafür bislang fehlt, obwohl die Notwendigkeit der Speicherung von allen Seiten anerkannt wird.

Urteil des BAG zur Schwerbehinderteneigenschaft

In seinem Urteil vom 18. September 2014 (8 AZR 759/13) hat das Bundesarbeitsgericht entschieden, dass ein schwerbehinderter Mensch, der bei seiner Bewerbung um eine Stelle den besonderen Schutz und die Förderung nach dem Sozialgesetzbuch (SGB) IX in Anspruch nehmen will, die Eigenschaft, schwerbehindert zu sein, grundsätzlich im Bewerbungsschreiben oder unter deutlicher Hervorhebung im Lebenslauf mitteilen muss. Eine solche Mitteilung müsse bei jeder Bewerbung erfolgen. Auf Erklärungen bei früheren Bewerbungen komme es nicht an.

Nach dem Datenschutzrecht liege es in der Entscheidung des schwerbehinderten Menschen, ob er die Schwerbehinderung bei der Bewerbung berücksichtigt haben will oder nicht.

Urteil des Bundesarbeitsgerichts zur dauerhaften Veröffentlichung eines Firmenvideos

Ein Mitarbeiter verlangte nach seinem Ausscheiden aus einem Unternehmen von seinem ehemaligen Arbeitgeber die Unterlassung der weiteren Veröffentlichung des Ausschnitts eines Videos zu Werbezwecken im Internet, auf dem er zu sehen war, sowie die Zahlung eines Schmerzensgeldes. Ursprünglich hatte er seine Einwilligung in die Filmaufnahmen erteilt. Nach Ausscheiden aus dem Betrieb wollte er die Einwilligung widerrufen. Er hat seinen Anspruch auf Sperrung auf § 35 Abs. 3 Bundesdatenschutzgesetz (BDSG) gestützt.

Das Bundesarbeitsgericht (BAG) hat die Abweisung der Anträge durch das Landesarbeitsgericht (LAG) Rheinland-Pfalz mit Urteil vom 11. Dezember 2014 (8 AZR 1010/13) bestätigt. Es hat klargestellt, dass der einschlägige Prüfungsmaßstab im Vorliegenden die §§ 22, 23 Kunsturhebergesetz (KUG) sind, die dem BDSG vorgehen. Auf die Auffangfunktion des BDSG könne nicht, auch nicht hilfsweise oder ergänzend, zurückgegriffen werden. Auch auf etwa strengere gesetzliche Voraussetzungen des BDSG könne grundsätzlich nicht verwiesen werden. Allerdings sei das KUG verfassungskonform auszulegen. Verfassungsgrundsätze, die zum Datenschutzrecht und dem BDSG geführt haben, seien bei der Anwendung des KUG zu beachten und zu wahren. Wegen der Bedeutung des Rechts der Arbeitnehmer, auch im Arbeitsverhältnis ihr Grundrecht auf informationelle Selbstbestimmung ausüben zu dürfen, führe dies dazu, dass im Arbeitsverhältnis die Einwilligung in Filmaufnahmen der Schriftform bedürfe. Nur dadurch könne verdeutlicht werden, dass die Einwilligung der Arbeitnehmer in die Veröffentlichung ihrer Bildnisse unabhängig von den jeweiligen Verpflichtungen aus dem eingegangenen Arbeitsverhältnis erfolgt und dass die Erteilung oder Verweigerung der Einwilligung für das Arbeitsverhältnis keine Folgen haben dürfe. Auch im Rahmen eines Arbeitsverhältnisses könnten Arbeitnehmer sich grundsätzlich frei entscheiden, wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben wollen. Dem stehe weder die grundlegende Tatsache, dass Arbeitnehmer abhängige Beschäftigte sind, noch das Weisungsrecht des Arbeitgebers entgegen. Mit der Eingliederung in einen Betrieb begäben sich die Arbeitnehmer nicht ihrer Grund- und Persönlichkeitsrechte. Eine Ne-

benpflicht des Arbeitsnehmers aus dem Arbeitsverhältnis, der Erhebung, Verarbeitung und Veröffentlichung seiner Daten zuzustimmen, bestehe nicht. Allerdings könne eine einmal erteilte Einwilligung nicht allein aus Anlass der Beendigung des Arbeitsverhältnisses widerrufen werden. Es seien Rücksichtnahmepflichten gegenüber dem Arbeitgeber zu beachten. Im Rahmen der durchzuführenden Gesamtabwägung sei zu berücksichtigen, um welche Art von Video es sich handele. Bei Firmenvideos, bei denen es nicht namentlich um einzelne hervorgehobene Arbeitnehmer geht, sondern nur um das Unternehmen an sich, könne der einzelne Arbeitnehmer nicht mehr beliebig seine Einwilligung zurückziehen.

Dieses Urteil bietet m. E. einen sachgerechten Ausgleich zwischen dem Bildnisschutz der Arbeitnehmer auf der einen und den unternehmerischen Interessen des Arbeitgebers auf der anderen Seite. Es bestätigt auch mein Votum aus dem Jahr 2011 zur Frage der Zulässigkeit von Fotos und Videos von **rbb**-Mitarbeitern im Internet. Schon damals hatte ich votiert, dass dafür grundsätzlich die Einwilligung der Dargestellten erforderlich ist. Die Ausnahmen ergeben sich aus § 23 Kunsturhebergesetz (z. B. „zeitgeschichtliches Ereignis", „Beiwerk zur Landschaft", „Teilnahme an öffentlichen Aufzügen"). Bei Mitarbeiterinnen und Mitarbeitern, deren Bildnisdarstellung in den Medien zu ihrem Berufsbild gehört (z. B. Fernsehmoderatoren), ist von dem konkludenten Einverständnis durch Abschluss eines entsprechenden Vertrages (Arbeitsvertrag bzw. Honorarvertrag) mit dem **rbb** auszugehen.

III. Berlin

Evaluation Rundfunkbeitragsstaatsvertrag

Zu dem am 1. Januar 2013 in Kraft getretenen Rundfunkbeitragsstaatsvertrag (RBStV) hatten die Länder in einer Protokollnotiz eine Evaluierung des neuen Finanzierungsmodells vereinbart. Die Evaluierung umfasst insbesondere die Entwicklung der Erträge aus dem Rundfunkbeitrag und die jeweiligen Anteile der privaten Haushalte, der Privatwirtschaft und der öffentlichen Hand am Gesamtertrag. Dabei werden auch die Notwendigkeit und Ausgewogenheit der Anknüpfungstatbestände geprüft. Entsprechend der Forderung einiger Landtage werden im Zuge der noch

andauernden Evaluierung auch die bisherigen Bestimmungen zum Datenschutz geprüft.

Am 21. Oktober 2014 fand eine Besprechung in Berlin statt, an der Vertreter der Länder und der Rundfunkanstalten, ein Vertreter des Zentralen Beitragsservices sowie die Datenschutzbeauftragten der Länder und der Rundfunkanstalten teilgenommen haben. Ziel des Gesprächs war es, sich über die bisherigen Erfahrungen mit den datenschutzrelevanten Regelungen des Rundfunkbeitragsstaatsvertrags auszutauschen und etwaige Problemfelder und mögliche Verbesserungsbedarfe anzusprechen. Der Vertreter des Zentralen Beitragsservices äußerte die Notwendigkeit, einen weiteren umfassenden Meldedatenabgleichs durchzuführen. Außerdem wurde über die mögliche Verlagerung datenschutzrechtlicher Bestimmungen aus der Satzung in den Staatsvertrag und die Verlängerung des Verbotes, Adressen privater Personen anzumieten, diskutiert. Die Vertreter der Rundfunkanstalten äußerten den Wunsch nach einer klarstellenden Rechtsgrundlage für die Verarbeitung von Telekommunikationsdaten im nichtprivaten Bereich.

Die im Nachgang eingereichte schriftliche Stellungnahme der Rundfunkdatenschutzbeauftragten vom 31. Januar 2015 ist als Anlage diesem Bericht beigefügt. Unser Resümee der Umstellung von der gerätebezogenen Rundfunkgebühr auf den wohnungsbezogenen Rundfunkbeitrag fällt positiv aus. Durch sie sind Nachforschungen zu den Wohnverhältnissen und zur Ausstattung mit Rundfunkempfangsgeräten obsolet geworden. Im Zuge der Umstellung gab es vergleichsweise wenige Datenschutzbeschwerden.

Die Hauptkritik in der Bevölkerung richtete sich erkennbar nicht gegen die Datenschutzbestimmungen im RBStV, sondern gegen dessen Grundlagen und Struktur, mit denen sich inzwischen unter anderem der Verfassungsgerichtshof Rheinland-Pfalz in seiner Entscheidung vom 13. Mai 2014 (VGH B 35/12) und der Bayerische Verfassungsgerichtshof in seinen Entscheidungen vom 15. Mai 2014 (Vf- 8-VII-12, 24-VII-12) beschäftigt und die Verfassungsmäßigkeit der Regelungen festgestellt haben. Der Bayerische Verfassungsgerichtshof hat sich in seinen Entscheidungen auch ausführlich mit den Anzeige- und Nachweispflichten in § 8 in Verbindung mit

§ 9 Abs. 2 Satz 1 Nr. 1 und 3 RBStV und mit dem einmaligen Meldedatenabgleich nach § 14 Abs. 9 RBStV auseinandergesetzt und auch diese Regelungen für mit der Bayerischen Verfassung vereinbar erklärt. Auch das Berliner Verwaltungsgericht hatte mit Beschluss vom 22.5.2013 in einem Eilverfahren den Einmaligen Meldedatenabgleich für zulässig erklärt (VG 27L64.13). Der Beschluss ist vom OVG Berlin-Brandenburg mit Beschluss vom 6.8.2013 bestätigt worden (OVG 11 S 23.13).

Aus Sicht der Rundfunkdatenschutzbeauftragten haben die Rundfunkanstalten überzeugend dargelegt, dass allein die staatsvertraglichen Anzeigepflichten und Auskunftsrechte nicht ausreichen, um einer erneuten Erosion des Teilnehmerbestandes wirksam vorzubeugen. Eine Verschlechterung des Datenbestandes ist insbesondere in den Fällen zu erwarten, in denen die bisherige Beitragszahlerin oder der bisherige Beitragszahler verstirbt oder umzieht. Trotz der gesetzlichen Anzeigepflicht des in der Wohnung verbleibenden Gesamtschuldners erhalten in vielen Fällen die Rundfunkanstalten bzw. der Zentrale Beitragsservice keine Information darüber, wer für die entsprechende Wohnung als (neue/r) Beitragspflichtige/r angeschrieben werden kann. Auch von einem „Hineinwachsen" Jugendlicher in die Beitragspflicht erhält der Beitragsservice oftmals keine Kenntnis. Wir haben daher die Durchführung eines wiederholten vollständigen Meldedatenabgleich befürwortet. Er ist nach unserer Überzeugung das mildeste und am besten geeignete Mittel, um einer Erosion des Teilnehmer-Datenbestandes, die zu einem Vollzugsdefizit und einer damit verbundenen ungleichen wirtschaftlichen Belastung der Beitragsschuldner führen würde, vorzubeugen. Die Rundfunkdatenschutzbeauftragten haben sich auch dafür ausgesprochen, dass im nicht privaten Bereich eine ausdrückliche Rechtsgrundlage für die Erhebung und Nutzung von allgemein zugänglichen Telefonnummern und E-Mail-Adressen geschaffen wird, damit der Beitragsservice die Möglichkeit hat, Sachverhalte per Telefon bzw. per Mail aufzuklären, wenn auf schriftliche Anfragen nicht reagiert wird. Im Unterschied zu Privatpersonen wird die in den Landesdatenschutzgesetzen erlaubte Nutzung von Daten aus allgemein zugänglichen Quellen im Geschäftsverkehr auch nicht durch Regelungen über unzumutbare Belästigungen eingeschränkt (§ 7 UWG). Ein Pilotversuch zur Sachverhaltsaufklärung im nicht privaten Bereich auf diesem Weg ist erfolgreich verlaufen. Schließlich würden wir es im Sinne der Normenklarheit begrüßen, wenn die bisher in

§ 7 der Satzung des Rundfunk Berlin-Brandenburg über das Verfahren zur Leistung der Rundfunkbeiträge (Rundfunkbeitragssatzung) enthaltenen Regelungen über die Datenerhebung bei öffentlichen Stellen in den Rundfunkbeitragsstaatsvertrag überführt würden.

C. Datenschutz und Datensicherheit im rbb

I. Allgemeines

1. Dienstanweisung zur Auftragsdatenverarbeitung

2011 ist das Berliner Datenschutzgesetz novelliert worden. Dabei sind insbesondere die in § 3 definierten Anforderungen an die Auftragsdatenverarbeitung verschärft und an die entsprechende Regelung im Bundesdatenschutzgesetz angepasst worden.

Zwar existieren seit einigen Jahren die **rbb**-Wartungsrichtlinien, die die Auftragsdatenverarbeitung in diesem Bereich regeln. Dieses Regelungswerk wurde 2012 an die verschärfte Rechtslage angepasst. Allerdings gibt es im **rbb** daneben eine Vielzahl anderer Auftragsdatenverarbeitungsverhältnisse, wie z. B. das Hosting von Internet-Angeboten, die Bearbeitung der Beihilfeanträge, Dienstleistungen im Zusammenhang mit der Medienforschung und das Cloud Computing. Daher benötigen wir dringend eine allgemeine Dienstanweisung zur Auftragsdatenverarbeitung. Seit 2012 haben die OUI und ich von der Geschäftsleitung den Auftrag, einen Entwurf für eine entsprechende Dienstanweisung zu erarbeiten. Inzwischen liegt der Geschäftsleitung unser mit allen Bereichen abgestimmter Entwurf vor.

2. IT-Sicherheitskreis

Wie im vergangenen Tätigkeitsbericht erwähnt, ist die Dienstanweisung zur Gewährleistung der IT-Sicherheit am 23. April 2014 in Kraft getreten. 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. Der ISK setzt sich aus sog. Bereichs-Informationssicherheitsbeauftragten zusammen, die von den vier Direktionen, der OUI sowie der Hauptabteilung Technik und Betrieb entsandt sind. Außerdem gehören dem ISK eine Vertreterin bzw. ein Vertreter des Personalrats, die Datenschutzbeauftragte und in beratender Funktion ein Vertreter der Revision an.

Am 1. Juni 2015 hat der ISK zum ersten Mal getagt. Erörtert wurden die Aufgaben und die Struktur des ISK. Dabei hat sich gezeigt, dass die Dienstanweisung an verschiedenen Stellen überarbeitet werden muss. Die Freienvertretung sollte ebenfalls am ISK teilnehmen. Die Mitglieder kamen überein, dass eine Abstimmung und Entscheidung bei sicherheitskritischen Vorfällen – wie in der Dienstanweisung derzeit vorgesehen - zum Teil nicht den fachlichen Kompetenzen der Teilnehmerinnen und Teilnehmern entspricht und im Ernstfall zu lange dauern würde. Anstatt dessen sollen die Mitglieder des ISK über sicherheitskritische Vorfälle lediglich informiert werden. Außerdem sollen diese innerhalb des ISK ausgewertet werden.

Außerdem hat der IT-Sicherheitsbeauftragte einen Überblick über die Dokumente zur Informationssicherheit im **rbb** gegeben und die aktuelle Sicherheitslage erläutert.

Der ISK wird sich künftig vier Mal im Jahr treffen, um Fragen zur Informationssicherheit zu erörtern.

3. Software zum IT-Sicherheitsmanagement

Gemäß § 19 a Abs. 1 Satz 4 Berliner Datenschutzgesetz (BLDSG) führt die behördliche Datenschutzbeauftragte die Beschreibungen und Verzeichnisse nach § 19 BLDSG.

In der Gemeinschaftseinrichtung IVZ setzt die Informationssicherheitsbeauftragte die Software verinice für das Informationssicherheits-Management ein. In diesem System ist auch ein elektronisches Dateienverzeichnis enthalten. Die Informationssicherheitsbeauftragte hat einer Vertreterin der OUI und mir dieses Tool im Frühjahr 2015 vorgeführt. Ich würde die Anschaffung für den **rbb** sehr begrüßen - nicht nur, weil ich von dem elektronischen Dateienverzeichnis unmittelbar profitieren würde, sondern auch weil ich die systematische Erfassung der gesamten im **rbb** eingesetzten Hard- und Software einschließlich der verarbeiteten Daten nebst Angabe zum Schutzbedarf für das IT-Sicherheitsmanagement für unerlässlich halte. Allerdings bedeutete der Einsatz dieses Tools in der Anfangsphase zunächst einmal einen relativ hohen administrativen Aufwand. Die OUI befindet sich noch in einer Geeignetheitsprüfung.

4. Dienstanweisung für die Nutzung von IT

Im **rbb** fehlt bislang auch eine Dienstanweisung, die die Nutzung von PC und mobilen Endgeräten einheitlich regelt. In der OUI wird derzeit ein entsprechender Entwurf in Abstimmung mit mir erarbeitet.

5. SAP-Dienstvereinbarungen

a) Aktualisierung der SAP-Dienstvereinbarungen

In den Verhandlungen mit dem Personalrat zu den aktualisierten SAP-Dienstvereinbarungen sind umfangreiche Datenschutzschulungen vereinbart worden. Zum überwiegenden Teil dauern die Verhandlungen zu den einzelnen SAP-Modulen immer noch an. Nur die neue Dienstvereinbarung HCM ist bereits abgeschlossen.

Die gleichzeitige Einführung eines elektronischen Formulars, mit dem die Nutzungsberechtigung für SAP-Systeme beantragt und vom Personalrat genehmigt werden muss, führt seit Herbst 2014 dazu, dass bei mir regelmäßig Kolleginnen und Kollegen vorstellig werden, die sehr zeitnah im Datenschutz geschult werden müssen. Ihre Anträge waren zuvor vom Personalrat mit dem Hinweis, dass sie nicht im Datenschutz geschult seien, abgelehnt worden. Ich habe die Kolleginnen und Kollegen bislang jeweils einzeln bzw. so es möglich war auch in Kleingruppen geschult. Nunmehr soll ein Konzept für die Datenschutzschulungen erarbeitet werden, das den unterschiedlichen Bedürfnissen der Mitarbeiterinnen und Mitarbeiter (terminlich und inhaltlich) Rechnung trägt.

Eine ähnliche Regelung zu Datenschutzschulungen wie in SAP-HCM ist derzeit für die Module SAP-KMH und SAP-FI vor der Einigungsstelle strittig. Ich halte es nicht für sinnvoll, eine ausformulierte Datenschutzschulung starr vertraglich festzulegen. Genau dies fordert aber der Personalrat. Hier sind meinerseits auch Zweifel angebracht, ob eine derartige Forderung des Personalrats der Mitbestimmung unterliegt. Ferner sind durch die Module eBAR und BANF erheblich mehr Mitarbeiterinnen und Mitarbeiter zu schulen, so dass neue Formen für regelmäßige Datenschutzschulungen gefunden werden müssen. Ich plädiere in diesem Zusammenhang nachdrücklich für die Einführung von Online-Schulungen (eLearning). Nur so können Datenschutzschulungen (insbesondere Grundschulungen und Massenschulungen für eBAR und BANF) zeitnah, terminunabhängig und für viele Mitarbeiterinnen und Mitarbeiter in einem akzeptablen Zeitraum durchgeführt werden.

Im Zusammenhang mit der Dienstvereinbarung SAP-KMH wurden vom Personalrat der Inhalt der Formulare für freie Beschäftigte datenschutzrechtlich hinterfragt. Die Formulare sind zu überarbeiten und auf Grund des nun in Kraft getretenen Freienstatutes auch mit der Freienvertretung zu verhandeln. Ich habe wiederholt meine Unterstützung dazu angeboten.

b) Umsetzung der SAP-Dienstvereinbarungen

Die in den SAP-Dienstvereinbarungen vereinbarten Löschfristen für personenbezogene Daten sollen nunmehr umgesetzt werden. Auf meine jüngste Nachfrage zu diesem Thema gab es vor kurzem eine Besprechung, an der verantwortliche Mitarbeiter der HA Personal und OUI teilnahmen. Es wurde vereinbart, dass die HA Personal der OUI eine aktuelle Löschliste übermittelt. Das ist mittlerweile geschehen. Ende August soll nun noch ein finales Treffen mit einem externen Experten stattfinden und danach, also Ende des III. Quartals 2015, sollen endlich die Löschungen erfolgen.

6. Konzeption von Technischen Betriebsräumen

Wie berichtet hat eine Prüfung der Serverräume durch die Revision im Herbst 2011 ergeben, dass die technischen und organisatorischen Maßnahmen zur Sicherheit der Serverräume im **rbb** nicht vollständig den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen.

Daraufhin wurde seinerzeit ein Projektteam mit der Erarbeitung von Vorschlägen zur Optimierung der physikalischen Sicherheit beauftragt. Ich konnte die Belange des Datenschutzes in die entsprechenden Planungen einbringen. Allerdings sollte die Umsetzung in einem separaten Projekt erfolgen.

Von Dezember 2012 bis April 2013 führte der Rechnungshof von Berlin eine Prüfung des Einsatzes von Informationstechnik (IT) im Verwaltungsbereich des **rbb** durch. Dabei wurden die Feststellungen der Revision bestätigt. Am 12.6.2014 hat

der Leiter der OUI daraufhin zu einem Gespräch geladen, an dem auch die Leiterin der Hauptabteilung Gebäudemanagement teilnahm. Es wurde beschlossen, zunächst die sendenahen Betriebsräume zu identifizieren, um dann konkrete Maßnahmen zu ergreifen. Inzwischen gibt es eine neue Entwicklung:

Im Zuge einer für 2015 geplanten Ausschreibung der Sicherheitsdienstleistungen hat die Geschäftsleitung in Abstimmung mit dem Verwaltungsratsvorsitzenden entschieden, dass die Verträge zunächst um zwei Jahre verlängert werden, um in dieser Zeit ein technisches Sicherheitskonzept für die Liegenschaften des **rbb** zu erstellen. Ziel dieses Konzeptes ist die Reduzierung der permanenten Bewachungskosten durch technische Maßnahmen. Der noch zu beauftragende externe Berater wird für das Konzept insbesondere die Zutrittsbedingungen und Schließsysteme / Schlüsselverwaltung analysieren. Ich gehe davon aus, dass sich daraus auch konkrete Empfehlungen für die Serverräume und die technischen Betriebsräume ergeben werden. Das Sicherheitskonzept soll 2016 erstellt werden, damit die Rahmenbedingungen für die Ausschreibung 2017 feststehen.

7. Erstellung eines IT-Sicherheitskonzepts für mobile Endgeräte

Im **rbb** sind inzwischen über 500 dienstliche mobile Endgeräte in Benutzung (iPhones und iPads). Bei Beantragung eines mobilen Endgerätes werden den Nutzern die Nutzungsbedingungen ausgehändigt. Die Einhaltung der Nutzungsbedingungen muss von den Nutzern schriftlich bestätigt werden. Erst danach wird das beantragte Gerät konfiguriert und den Nutzern ausgehändigt.

Die bisherige Politik im **rbb** hinsichtlich der Geräte ist sehr liberal. So gibt es beispielsweise keine sog. white list, auf der sich die vom **rbb** zugelassenen Apps befinden, obwohl bekannt ist, dass bestimmte Apps aus dem Apple ITunes-Store Daten übermitteln können (z. B. Adressbuch, Standort, Fotos usw.). Der **rbb** weist jedoch auf diesen Umstand hin und sensibilisiert die Nutzer entsprechend. Zudem ist die Übertragung von dienstlichen Daten in externe Online-Datenspeicher (Cloud-Services, Dropbox, iCloud etc.) ausdrücklich untersagt.

Entsprechend einer seit längerem erhobenen Forderung von mir ist im Sommer dieses Jahres die Erstellung eines IT-Sicherheitskonzeptes für mobile Endgeräte sowie einer Richtlinie zur Nutzung der Geräte im Rahmen des **rbb**-Sicherheitskonzeptes extern beauftragt worden.

8. Das Unternehmens- und Historische Archiv (UHA)

Zum 1. Januar 2014 wurde im **rbb** das Unternehmens- und Historische Archiv (UHA) gegründet. Dem Beschluss der Geschäftsleitung ging eine dreijährige Projektphase voraus. Das Archiv agiert in der Verantwortung der HA Unternehmensentwicklung. Den neuen Umgang mit den Aktenbeständen soll die Neufassung der Dienstanweisung für die Bearbeitung und Verwaltung von Dokumenten und Akten regeln. Alle darüber hinausgehenden Nutzungsmodalitäten soll die „Benutzungsordnung für das Unternehmens- und Historische Archiv“ enthalten. An der Über- bzw. Erarbeitung dieser beiden Regelungswerke habe ich im Sommer 2014 mitgewirkt, da auch datenschutzrechtliche Aspekte eine Rolle spielen. Die Regelungswerke befinden sich **rbb**-intern noch in der Abstimmung.

9. Nutzungsbedingungen und Datenschutzhinweis für das neue „Suche & Biete“ im rbb-Intranet

Im Zuge des für den Herbst 2015 geplanten Relaunches des **rbb**-Intranets wird es auch eine neue „Suche & Biete“-Plattform geben. Es ist vorgesehen, dass die Nutzer ihre Anzeigen selbständig einstellen, bearbeiten, verwalten und löschen können. Die Nutzer gelangen über ein Login in ihren persönlichen Bereich, in dem sie Angebote erstellen und hier auch Bilder und Dokumente hinterlegen können. Die jetzigen Nutzungsregeln des Forums müssen dementsprechend angepasst werden. An der Überarbeitung war ich beteiligt. Dabei habe ich daraufhin gewirkt, dass das Verbot der Nutzung privater Datenträger an den PC-Arbeitsplätzen zur Vermeidung der Einschleusung von Viren in unser **rbb**-Datennetz auch hier beachtet wird. Aus diesem Grund erfolgt der Hinweis, dass Bilder über **rbb**-Hardware erstellt bzw. eingestellt werden können. Für den Fall, dass die Mitarbeiterinnen und Mitarbeiter keine rbb-Hardware nutzen können, wird empfohlen, die Bilder per eMail vom Smartphone oder Tablet zu verschicken und vom **rbb**-Account abzurufen.

10. Neues Gästemanagement-Tool bei Fritz

Die Veranstaltungen der Radiowellen, zu denen jeweils mehrere tausend Einladungen verschickt werden, bedürfen eines umfangreichen Gästelisten-Managements, da es üblicherweise verschiedene Gruppen und Zugangsberechtigungen gibt (geladene Gäste/VIP, Gewinner, Gäste der teilnehmenden Künstler, Fachpublikum und Pressevertreter u.a.). Der Musikchef der Radiowelle **Fritz** wandte sich im Frühjahr 2015 an das Justitiariat mit der Frage, ob aus juristischer Sicht etwas dagegen spricht, ein Gästelisten-Management-Tool einzusetzen, mit dem z. B. die namentliche Registrierung, Zuordnung zu bestimmten Zugängen am Einlass und statistische Auswertungen möglich seien. Das Tool würde **Fritz** nahezu kostenfrei angeboten. Das Justitiariat hat mich aufgrund der datenschutzrechtlichen Relevanz in diesen Vorgang mit einbezogen.

In einem Gespräch erläuterte ich dem Musikchef, dass es für eine datenschutzrechtliche Prüfung erforderlich sei, das konkrete Konzept zu kennen. Welche Funktionen des Tools würden genutzt und welche personenbezogenen Daten der Gäste wie, wo und durch wen verarbeitet werden? Der Anbieter müsste dem **rbb** ein Informationssicherheitskonzept zur Verfügung stellen. Den Verantwortlichen stehe ich auch in dieser Sache weiterhin für eine Prüfung zur Verfügung.

11. Arbeitnehmerüberlassung von Mitarbeitern der rbb media

Im Frühjahr 2014 erfuhr ich davon, dass der **rbb** mit Wirkung seit 1. Februar 2014 zur Unterstützung des IT-Supports Mitarbeiterinnen und Mitarbeiter der **rbb** media ausgeliehen hatte. Auf meinen Anstoß hin wurde die datenschutzrechtliche Unterweisung nachgeholt und von allen Mitarbeiterinnen und Mitarbeitern eine Vertraulichkeitserklärung eingeholt.

Gleichzeitig wurden auch die festangestellten Mitarbeiter des IT-Services auf den aktuellen Stand in Sachen Datenschutz und Datensicherheit gebracht.

12. Druck von Visitenkarten

Im Sommer 2014 wandte sich die Abteilung Einkauf an mich mit dem Anliegen, die bisherige manuelle Bestellung von Visitenkarten bei einer externen Druckerei auf ein EDV-gestütztes Bestellsystem umzustellen. Für die Gestaltung des Workflows sollte dem Auftragnehmer eine Kostenstellenliste mit allen Angaben zu den **rbb**-internen Kostenstellen und Genehmigungswegen zur Verfügung gestellt werden. Ich habe dies moniert und die Frage aufgeworfen, ob nicht eine Lösung vorstellbar sei, bei der die **rbb**-Interna nicht offengelegt werden müssen. Der Einkauf hat sich auf den Standpunkt gestellt, dass eine derartige Lösung wesentlich aufwändiger und teurer sei. Nach eingehenden Diskussionen, an denen auch die Revision teilnahm, hat der Einkauf aus Gründen der Wirtschaftlichkeit sein Vorhaben abgebrochen. Bis auf weiteres führt er die Bestellungen weiterhin manuell durch.

13. Datenschutzrechtliche Beschwerde über die Service-Redaktion

Die Service-Redaktion ist die Stelle im **rbb**, die telefonische Zuschaueranfragen und –beschwerden entgegen nimmt und bearbeitet.

Ein Zuschauer hatte sich bei mir über die vermeintliche Praxis der Service-Redaktion beschwert, dort eingehende Anrufe mitzuschneiden. Als Indiz nannte er die Aussage einer Mitarbeiterin der Service-Redaktion: „Sie haben doch schon mehrmals wegen dieses Themas bei uns angerufen."

Ich habe mich daraufhin bei der Service-Redaktion noch einmal zur dortigen Praxis erkundigt. Mir wurde bestätigt, dass dort das mit mir abgestimmte Verfahren praktiziert wird: Wird von Anrufern um Stellungnahme oder Rückruf gebeten, erfasst die Service-Redaktion die Kontaktdaten für den jeweiligen Vorgang. Nach Bearbeitung des jeweiligen Anliegens werden die zu dem Anruf gespeicherten personenbezogenen Daten gelöscht. Die Anrufe und Gesprächsgegenstände selbst bleiben zu internen Zwecken im System der Service-Redaktion anonymisiert gespeichert. Da es nahezu immer der Beschwerdeführer war, der sich zu einem bestimmten Thema am Telefon geäußert hatte, konnten die Mitarbeiterinnen und Mitarbeiter diese anonymisierten Anrufe im System ohne weiteres dem Beschwerdeführer zuordnen.

II. Aktuelle IT-Projekte

1. Regeltermin IT-Projekte

In regelmäßigen Terminen informiert OUI 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. Ich würde es begrüßen, wenn auch die Freienvertretung zukünftig an den Treffen teilnehmen könnte und das Themenspektrum auf sämtliche IT-Projekte im **rbb** erweitert würde. Dies bedeutete eine Einbeziehung von Be-

reichen innerhalb der Produktions- und Betriebsdirektion. Im Berichtszeitraum fanden Termine am 27. Mai, 27. Juni und 13. Oktober 1014 statt.

2. Dispositionssysteme

In meinen früheren Berichten hatte ich wiederholt über die Verhandlungen über die Einführung eines neuen Dispositionssystems zwischen Geschäftsleitung und Personalrat berichtet. Diese Verhandlungen, an denen ich beteiligt war, endeten Anfang 2012 mit einer Entscheidung durch die Einigungsstelle. Leider konnte das System am Ende aus technischen Gründen nicht in Betrieb gehen.

In den Bereichen HF-Betrieb/Produktion und **Info**radio wurde seit vielen Jahren ein anderesDispositionssystem zur Sachmittel- und Personaldisposition eingesetzt. Nachdem der Lieferant der ursprünglichen Software im Jahr 2012 den **rbb** darüber informiert hatte, dass keine Weiterentwicklungen bzw. Fehlerbehebungen am Quellcode der Software mehr durchgeführt würden und sich die geplante Ablösung durch das neue System zerschlagen hatte, hat sich der **rbb** entschlossen, übergangsweise eine eigenprogrammierte Software namens Malu zu nutzen, welche die Grundfunktionalitäten des ursprünglichen Systems 1:1 abbildet. Die Software wurde ab Oktober 2014 eingeführt. Sie wurde in enger Zusammenarbeit mit der Hörfunk-Produktion erstellt, getestet und optimiert.

Vor der Implementierung dieser Übergangslösung habe ich auf der Basis eines durch den IT-Sicherheitsbeauftragten genehmigten IT-Sicherheitskonzepts eine Vorabkontrolle durchgeführt.

Inzwischen gibt es ein neues Projekt mit dem Ziel, eine bereits bei HR und SWR befindliche Software auch für die Disposition des **rbb** nutzbar zu machen. Nach der Produktivsetzung wird das System MIRAAN zunächst von Disponentinnen und Disponenten bei Inforadio, im Hörfunkbetrieb, bei **kultur**radio, in der Zentraldisposition, in der Abteilung Bild und im ARD-Hauptstadtstudio genutzt. Anschließend ist ein Einsatz in weiteren disponierenden Bereichen im **rbb** möglich. Ich werde in die Vorbereitungsarbeiten wie üblich einbezogen und werde vor Beginn des Probebetrie-

bes die abschließende Vorabkontrolle durchführen. Hinsichtlich der Dokumentation habe ich mich mit dem Projektleiter darauf geeinigt, dass wir uns an der Struktur der vor der Einigungsstelle im Jahr 2012 verhandelten Dokumente orientieren.

3. 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 Vertreter des Personalrates, des Bereichs OUI und der Referent für Dienstvereinbarungen 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. Bislang habe ich die elektronischen Antragsformulare für die SAP-Nutzung und für die Anforderung von Hardware geprüft und für datenschutzkonform erklärt. Ein weiteres eFormular „Antrag auf Ausstellung einer Studentenvereinbarung" befindet sich aktuell in der Prüfung.

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

Im letzten Tätigkeitsbericht hat Herr Dr. Bismark über den Stand des Projektes eines multimedialen Redaktions- und Planungssystem für die Programmbereiche Fernsehen, Hörfunk und Online informiert. Seit einiger Zeit läuft der Probebetrieb. Ich wurde von Anfang an über die Ausgestaltung und die Fortschritte bei der Entwicklung des Systems regelmäßig unterrichtet und habe insbesondere das Datenschutzkonzept einschließlich des Berechtigungskonzepts und Aspekte der IT-Sicherheit begutachtet. Für eine abschließende Vorabkontrolle vor Beginn des Regelbetriebs fehlt allerdings die von Anfang an eingeforderte vollständige Auflistung aller personenbezogenen Daten, die im System verarbeitet werden, mit Angabe des Verwendungszwecks, der Aufbewahrungsdauer, der Angabe, wer auf die Daten zugreifen darf, welche Schnittstellen es gibt sowie Angaben zu den Löschfristen.

Schließlich muss auch die Rechtsgrundlage für die Verarbeitung der Daten im Einzelnen angegeben werden.

5. Unified Communications

Unified Communications (UC) steht für „vereinheitlichte Kommunikation“ und beschreibt die Integration von Kommunikationsmedien in einer einheitlichen Anwendungsumgebung. Die Idee hinter Unified Communications ist, durch eine Zusammenführung aller Kommunikationsdienste die Erreichbarkeit von Kommunikationspartnern in einer verteilten Arbeitswelt zu erhöhen und so geschäftliche Prozesse zu verbessern.

Hinter UC verbergen sich neben der klassischen Sprachkommunikation auch Konferenzplattformen, Methoden zur Integration von Kommunikation in Applikationen, und Messaging-Komponenten, wie E-Mail u.a., die den Wissensaustausch und die Integration dieser verschiedenen Kommunikationsmedien in einer einheitlichen IP-basierten Anwendungsumgebung unterstützen.

Im Frühjahr 2015 hat die OUI hat die Mitarbeitervertretungen und mich darüber informiert, dass sie in einem Vorprojekt die Möglichkeiten von UC ausloten wolle. Dabei wurde festgelegt, dass die führende **rbb**-Kommunikationsanwendung Lotus Notes sein solle. Alle zu testenden Dienste werden in Lotus Notes integriert und stehen dort zur Verfügung.

Ursprünglich war geplant, in einer gesonderten Umgebung ohne Verbindung zu den Produktivsystemen zu testen. Nachdem nun einige Zeit in einer gesonderten Umgebung getestet wurde, besteht seitens der Projektleitung der Wunsch, den Test auf die Produktivsysteme auszuweiten, um auch sämtliche Funktionen der Anwendung testen zu können. Die Projektleitung hat mich von der Notwendigkeit der Ausweitung des Tests auf die Produktivsysteme überzeugt. Zusätzlich zu den bisherigen Leistungsmerkmalen, die für den Telekommunikationsanlagenverbund einvernehmlich mit dem Personalrat und mir vor einigen Jahren festgelegt wurden, bietet UC einige ergänzende Leistungsmerkmale wie die Web Collaboration (inter-

aktives Desktop sharing), die Videotelefonie (wenn web cam vorhanden), das Anzeigen von „Präsenzinformationen" und der vereinfachter Aufbau von Sprachkonferenzen. Aus datenschutzrechtlicher Sicht sehe ich keinen generellen Hinderungsgrund für den Test dieser zusätzlichen Funktionen. Dabei müssen bestimmte Bedingungen wie die Freiwilligkeit – z. B. bei den Präsenzanzeigen – beachtet werden.

Bislang steht allerdings noch eine Bestätigung aus, dass die Datensicherheit der Produktivsysteme trotz der Durchführung des Tests gewährleistet ist. In diesem Fall habe ich darum gebeten, dass diese Bestätigung von einer unabhängigen Stelle eingeholt wird. Denn hier besteht zumindest theoretisch ein Interessenskonflikt, da der Informationssicherheitsbeauftragte zugleich der für das Projekt verantwortliche Bereichsleiter ist.

III. Beschäftigtendatenschutz

1. Bewerbermanagementsystem

Schon 2006 war die Einführung eines elektronischen Bewerbermanagementsystems geplant gewesen. Schon damals war es das Ziel, den Verwaltungsaufwand zu reduzieren und Kosten zu senken sowie auf das geänderte Bewerbungsverhalten zu reagieren. Der **rbb** hatte zu diesem Zweck eine komplette Dienstvereinbarung nebst Anlagen mit dem Personalrat ausgehandelt. In die Verhandlungen war ich seinerzeit einbezogen. Das geplante System kam aufgrund technischer Probleme allerdings nie zum Einsatz. Der Kauf wurde rückabgewickelt.

Nunmehr wird ein neuer Vorstoß unternommen, ein elektronisches Bewerbermanagementsystem beim **rbb** einzuführen. Die erarbeiteten Unterlagen und Erfahrungen aus dem Vorgängerprojekt fließen in das aktuelle Projekt ein und werden durch neue Erkenntnisse bzw. Anforderungen ergänzt, um nun im zweiten Anlauf eine gute Lösung zu erreichen.

Dem Anfang 2015 aufgenommenen Probebetrieb habe ich unter folgenden Bedingungen zugestimmt:

- Das externe Rechenzentrum in Nürnberg, wo die Daten gehostet werden, ist BSI- und ISO 27001 zertifiziert.

- Die Verbindung ist 2054-bit SSL verschlüsselt.

- In einem Berechtigungskonzept werden die Zugriffe in den verschiedenen Rollen definiert.

- Der Zugriff erfolgt eingeschränkt auf die für die jeweilige Rolle notwendigen Informationen mit Hilfe einer persönlichen Nutzerkennung.

- Die Daten werden nach 6 Monaten gelöscht. Es gibt keine Schnittstelle zu anderen Systemen.

- Der Zugriff ist ausschließlich über Rechner des **rbb** möglich.

2. Sicherere Unterbringung von Personalakten

Seit Jahren setze ich mich für eine Unterbringung von Personalakten in feuerfesten Schränken ein. Die derzeit im Fernsehzentrum stattfindende Schadstoff-Sanierung habe ich im Sommer 2014 zum Anlass für einen weiteren Vorstoß genommen. Erneut wurden von der Abteilung Infrastruktur Kostengründe ins Feld geführt. Die durch feuerfeste Schränke verursachten Mehrkosten seien im Projekt der Schadstoffsanierung nicht berücksichtigt. Außerdem würde es zu Terminverschiebungen für das Projekt kommen. Aus der Abteilung Bau, die neben der Abteilung Infrastruktur für die sichere Verwahrung von Akten zuständig ist, wurde mir folgendes zu meine Forderung erläutert: Im Zuge der Beseitigung von Brandschutzmängeln haben sich die Projektbeteiligten dafür ausgesprochen, eine Sprüh-Wasser-Nebel-Löschanlage einzubauen. Damit werden Mängel, die baulich nicht beseitigt werden können, kompensiert. Mit der Nebel-Anlage werde verhindert, dass ein Brand ent-

steht oder sich im Hochhaus ausbreitet. Mit dem Einbau der Nebel-Anlage könnten auch die vorhandenen Akten besser geschützt werden. Der Einbau soll bis 2016 abgeschlossen sein. Auch die Bauabteilung sieht jedoch ein verbleibendes Restrisiko für die Akten, denn bei einem Extremereignis kann niemand sicherstellen, dass physikalische Akten nicht doch vernichtet werden oder verloren gehen. Die Bauabteilung und ich sind uns deshalb einig darin, dass es anzustreben wäre, die Personalakten und weitere wichtige Dokumente – soweit noch nicht geschehen – zu digitalisieren.

3. Versand elektronischer Gehaltsabrechnungen

Die Gehaltsabrechnungen der festangestellten Mitarbeiterinnen und Mitarbeiter des **rbb** werden bislang innerhalb des **rbb** als Hauspost verteilt. Die Boten geben die verschlossenen Briefe in den Sekretariaten der einzelnen Abteilungen bzw. Bereiche ab. Die Sekretariate verteilen die verschlossenen Briefe anschließend auf die Postfächer der einzelnen Mitarbeiterinnen und Mitarbeiter. Bei erkennbarer längerer Abwesenheit werden die Briefe – wie auch die Honorarabrechnungen freier Mitarbeiterinnen und Mitarbeiter - per normaler Post an die Wohnadresse der Mitarbeiter verschickt. Bei nichtvorhersehbarer oder kürzerer Abwesenheit liegen die per Hauspost zugestellten Briefe mitunter einige Tage für Kolleginnen und Kollegen zugänglich in den Postfächern der Betroffenen.

Innerhalb der HA Personal gibt es die Überlegung, die Gehaltsabrechnungen künftig elektronisch zu versenden. Gedacht ist an einen Versand an die betriebliche E-Mailadresse. Ich habe dazu die Auffassung vertreten, dass diese Versendungsart aus datenschutzrechtlicher Sicht nicht zu beanstanden ist, wenn es ein entsprechendes IT-Sicherheitskonzept gibt. Im Gegenteil wäre die elektronische Versendung unter Einhaltung entsprechender Sicherheitsmaßnahmen aus meiner Sicht sogar eine Verbesserung im Vergleich zum bisherigen Verfahren. Ich habe daher angeregt, die Überlegungen beispielsweise auch auf Reisekostenabrechnungen auszuweiten, die wir derzeit nur auf Nachfrage erhalten.

Eine kleine Arbeitsgruppe aus Vertretern der HA Personal, des Informationsverarbeitungszentrums, der Revision und mir erarbeitet derzeit ein Konzept für die elektronische Versendung der Dokumente.

4. Mitarbeiterbefragung radioeins

Im Juni 2014 hat radio**eins** eine Befragung zur Mitarbeiterzufriedenheit bei radio**eins** durchgeführt. Da sämtliche Mitarbeiterinnen und Mitarbeiter der Radiowelle erreicht werden sollten – auch solche ohne eigenen E-Mail-Account beim **rbb** - konnte nicht das beim **rbb** übliche Umfragetool von Lotus Notes zum Einsatz kommen.

Da eine andere Software gefunden wurde, mit der ebenfalls die Anonymität der Umfrage gewahrt werden konnte und es zudem auf meine Anregung hin einen eindeutigen Hinweis auf die Freiwilligkeit der Teilnahme gab, konnte ich der Mitarbeiterbefragung zustimmen.

5. Überarbeitung der Fragebögen für freie Mitarbeiterinnen und Mitarbeiter

Auf der Sitzung des der Datenschutzbeauftragten von ARD, ZDF und DLR am 3./4.4.2014 in München wurde konstatiert, dass alle Landesrundfunkanstalten ihre von den freien Mitarbeiterinnen und Mitarbeiter auszufüllenden Fragebögen überprüfen müssen. Insbesondere die aufgrund der tariflichen Regelungen zur Honorierung erforderlichen Übermittlungen der Daten freier Mitarbeiterinnen und Mitarbei-

ter an andere Landesrundfunkanstalten bedürfen einer klareren Formulierung. Nachdem innerhalb des AK DSB bis zum Sommer keine Aktivitäten in dieser Hinsicht stattgefunden hatten, bin ich auf unsere HA Personal mit dem Anliegen zugegangen, zumindest im **rbb** eine Prüfung und ggf. Überarbeitung der Fragebögen vorzunehmen. In einem längeren Gespräch erläuterte ich Vertretern der HA Personal, worauf es bei der Überarbeitung ankäme. Danach ist im Einzelnen zu prüfen, ob die bislang erhobenen Daten tatsächlich (in allen Fällen) erforderlich seien. Der Verwendungszweck sei klarer als bislang zu definieren. In dem Gespräch zeichnete sich ein erheblicher Überarbeitungsbedarf ab. Die HA Personal hat mir zugesichert, dass sie sich dieser Aufgabe jetzt zeitnah annehmen werde. Da ich inzwischen innerhalb des AK DSB für die Beschäftigtendatenverarbeitung federführend zuständig bin, werde ich einen erneuten Vorstoß zur Vereinheitlichung der Fragebögen vornehmen.

6. Veränderte Regelung zur Abholung von Dienstfahrzeugen

Im Straßenverkehrsgesetz (StVG) ist im § 21 die Halterverantwortung für die Betreiber eines Fuhrparks festgeschrieben. Spezifiziert wird die Verantwortung als Halter oder Betreiber eines Fuhrparks zudem im § 31 der Straßenverkehrszulassungsordnung (StVZO). Aus der Halterverantwortung resultieren entsprechende Prüfpflichten des Halters. Aus diesem Grund händigt der Fahrdienst – in Abweichung von der früheren Regelung - seit 1. September 2014 die von ihm disponierten Dienstfahrzeuge ausschließlich gegen Vorlage eines auf die Selbstfahrerin/den Selbstfahrer ausgestellten Führerscheins für die jeweilige Fahrzeugkategorie aus. Bis dahin hatte der Fahrdienst regelmäßig lediglich einmalig bei der Beantragung der Selbstfahrgenehmigung das Vorhandensein eines gültigen Führerscheins kontrolliert. Im Führerschein werden die Gültigkeit und die Übereinstimmung des Passbilds mit der Fahrerin/dem Fahrer überprüft. Darüber hinaus werden keine persönlichen Daten erhoben oder gespeichert. Das veränderte Verfahren war mit mir im Vorfeld abgestimmt worden. Eine Information über das geänderte Verfahren für die Mitarbeiterinnen und Mitarbeiter erfolgte im Intranet.

7. Datenverarbeitung zum Zwecke der Aufdeckung von Straftaten im Beschäftigungsverhältnis

Ende 2014 konsultierte mich der Leiter der Revision und erkundigte sich nach den datenschutzrechtlich zulässigen Möglichkeiten der Datenverarbeitung zur Aufklärung von Straftaten bzw. von Verstößen gegen arbeitsrechtliche Pflichten. Konkret ging es um die Frage, unter welchen Voraussetzungen die Auswertung von Daten auf Kopierern/Druckern und PCs grundsätzlich in Frage kommen könnte. Dazu habe ich folgendes ausgeführt:

Einschlägig für die Frage der Zulässigkeit der Datenverarbeitung bei der Aufklärung von Straftaten ist § 36 Abs. 1 **rbb**-Staatsvertrag i. V. m. § 2 Abs. 2 Berliner Datenschutzgesetz i. V. m. § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz.

Danach dürfen personenbezogene Daten eines Beschäftigten nur unter folgenden Voraussetzungen verarbeitet werden:

- zu dokumentierende tatsächliche Anhaltspunkte,
- begründeter Verdacht einer Straftat im Beschäftigungsverhältnis
- Erhebung, Verarbeitung oder Nutzung der Daten ist erforderlich,
- schutzwürdiges Betroffeneninteresse überwiegt nicht,
- Art und Ausmaß der Datenverwendung ist im Hinblick auf den Anlass nicht unverhältnismäßig.

Zu beachten ist, dass verdeckte Massenscreenings unzulässig sind, wenn kein konkreter Verdacht gegenüber *jedem einzelnen Mitarbeiter bzw. jeder einzelnen Mitarbeiterin* besteht, dessen/deren Daten abgeglichen werden. Außerdem muss die Maßnahme verhältnismäßig sein. Bei der Abwägung sind die Schwere der Vorwürfe und das Interesse des **rbb** an der Aufklärung gegen die Grundrechte der Betroffene auf Datenschutz und der Schutz des Fernmeldegeheimnisses gegeneinander abzuwägen.

Zusammenfassend lässt sich festhalten, dass die Anforderungen an die Zulässigkeit einer derartigen Maßnahme sehr hoch sind. Steht lediglich ein Verstoß gegen arbeitsrechtliche Pflichten im Raum, dürften breiter angelegte Untersuchungen ohne konkrete Verdachtsmomente gegenüber den Betroffenen von vornherein als unverhältnismäßig eingestuft werden.

8. Abgleich der rbb-Beschäftigtendaten mit Terrorlisten auf der Grundlage von EU-Verordnungen

Der Autokonzern Daimler überprüft seit Dezember 2014 alle drei Monate, ob Mitarbeitende auf Terror-Sanktionslisten stehen. Auch andere Firmen tun dies bereits oder planen, es zu tun. Daimler steht auf dem Standpunkt, mit dieser Maßnahme werde EU-Recht umgesetzt.

Dieses haben die Datenschutzbeauftragten von ARD, ZDF und DLR zum Anlass genommen zu prüfen, ob für die Rundfunkanstalten die Pflicht zu einem solchen Abgleich besteht. Dies ist nicht der Fall. Zwar sind die einschlägigen EU-Verordnungen zur Terrorbekämpfung unmittelbar bindendes Gesetzesrecht und wenden sich nicht nur an Sicherheitsbehörden, sondern verpflichten im Prinzip alle „nach dem Recht eines Mitgliedstaats gegründeten oder eingetragenen juristischen Personen, Gruppen, Unternehmen und Einrichtungen“. Mit ihnen wird bezweckt zu vermeiden, dass Terroristen oder terroristische Organisationen wirtschaftlichen Ressourcen wie z. B. auch Arbeitsentgelte zur Verfügung gestellt werden. Allerdings ist in den Verordnungen nicht geregelt, was konkret getan werden muss, um den gesetzlichen Verpflichtungen nachzukommen. Es fehlt an Regelungen zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Diese wären aber notwendig für einen entsprechenden Datenabgleich. Auch die subsidiär heranzuziehenden landesgesetzlichen Regelungen bieten keine Rechtsgrundlage für den Datenabgleich. Allerdings nehmen die Banken nach den Vorschriften des Kreditwesengesetzes einen Abgleich vor, so dass die Mitarbeiterinnen und Mitarbeiter im Rahmen der Zahlungen von Vergütungen bzw. Honoraren dort bereits erfasst sind.

9. Datenzulieferung für Altersversorgungsgutachten für die KEF

Die Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten (KEF) hat im Sommer 2014 ein Dienstleistungsunternehmen mit der Erstellung eines Gutachtens zur betrieblichen Altersversorgung der öffentlich-rechtlichen Rundfunkanstalten beauftragt. Zu diesem Zweck wurden die Rundfunkanstalten aufgefordert, dem Unternehmen die versorgungsrelevanten personenbezogenen Daten aller Mitarbeiter zu übermitteln. Ich habe von der Datenübermittlung der HA Personal an das Unternehmen erst nachträglich erfahren und veranlasst, dass mit dem Unternehmen noch eine Vereinbarung zum Datenschutz geschlossen wurde. Darin ist u.a. geregelt, dass nur anonymisierte Daten an die KEF übermittelt werden und dass die Daten nach Beendigung des Auftrages vom Auftragnehmer fachgerecht gelöscht werden. Die Löschung ist dem **rbb** auf Anforderung zu belegen. Da der Auftrag jetzt abgeschlossen ist, habe ich die HA Personal darum gebeten, sich über die fachgerechte Löschung der Daten bei der Firma zu vergewissern. Außerdem habe ich die HA Personal vorsorglich gebeten, in einem etwaigen Wiederholungsfall zunächst zu prüfen, ob es für ein Altersversorgungsgutachten nicht ausreicht, von vornherein mit anonymen Daten zu arbeiten.

10. Datenverarbeitung bei der Baden-Badener Pensionskasse (bbp)

Wie schon im letzten Tätigkeitsbericht erwähnt, hat der **rbb** – wie auch alle anderen Landesrundfunkanstalten - die Baden-Badener Pensionskasse (bbp) mit der Abwicklung der Versorgungsleistungen nach dem Versorgungstarifvertrag beauftragt. Bei der 1998 von den Rundfunkanstalten gegründeten Einrichtung handelt es sich rechtlich um einen Versicherungsverein auf Gegenseitigkeit. Der Sitz der bbp befindet sich in Räumlichkeiten des SWR in Baden-Baden. Die Arbeitsplätze der bbp sind an das Kommunikationsnetzwerk des SWR angebunden.

Da es sich bei der Datenverarbeitung der bbp für die Rundfunkanstalten um Auftragsdatenverarbeitung handelt, haben alle Rundfunkanstalten im Sommer 2014 gleichlautende Vereinbarungen zur Auftragsdatenverarbeitung mit der bbp abgeschlossen.

Zum 1. Juli 2014 hat das Informationsverarbeitungszentrum (IVZ) das Hosting für die bbp von einer privaten Firma übernommen. Das IVZ wird als rechtlich unselbstständige Gemeinschaftseinrichtung von DW, DRadio, MDR, NDR, RB, **rbb**, SR und WDR betrieben**.** Im Ergebnis ist durch diese interne Lösung die Sicherheit der Versorgungsdaten für die ARD-Mitarbeiter erhöht worden. Ich habe frühzeitig angemahnt, dass es auch zwischen bbp und IVZ eine Vereinbarung zur Auftragsdatenverarbeitung geben muss. Da das IVZ rechtlich unselbstständig ist, kann es keine Verträge mit Dritten abschließen. Das führte dazu, dass der federführende **rbb** für das IVZ mit der bbp eine entsprechende Vereinbarung abschließen musste. Für mich bedeutet das ganz praktisch, dass ich in dieser Angelegenheit die Einhaltung des Datenschutzes auf beiden Seiten zu kontrollieren habe: auf Seiten der bbp und auf Seiten des IVZ. Leider konnte das IT-Sicherheitskonzept für das Hosting noch nicht abschließend von den Datenschutzbeauftragten freigegeben werden. Der ursprüngliche Entwurf ist auf unsere Anregung hin überarbeitet worden. Bis zum Herbst dieses Jahres soll die endgültige Fassung vorliegen.

Die bbp hat zum Januar 2015 einen eigenen Datenschutzbeauftragten bestellt, der eng mit den Datenschutzbeauftragten der Landesrundfunkanstalten zusammenarbeitet.

11. Neues Freienstatut

Seit ungefähr elf Jahren gibt es im **rbb** eine Freienvertretung, gewählt von der Freienversammlung. Seit dem Sommer 2014 nun gibt es eine institutionalisierte Vertretung arbeitnehmerähnlicher freier Mitarbeiterinnen und Mitarbeiter. Auf der Grundlage von § 34 des zum 1. Januar 2014 novellierten **rbb**-Staatsvertrags hat die Intendantin für die arbeitnehmerähnlichen Personen im Sinne von § 12 a Tarifvertragsgesetz das Freienstatut geschaffen. Das Statut, das zum 1. Juni 2014 in Kraft getreten ist, gibt der Freienvertretung nun einklagbare Rechte. Der **rbb** informiert die Freienvertretung über alle Entwicklungen, die arbeitnehmerähnliche Freie betreffen. Die Freienvertretung kann Stellung beziehen u. a. bei Fragen des Arbeits- und Gesundheitsschutzes, der Gestaltung von Arbeitsplätzen, allgemeinen

Fragen der Fortbildung freier Mitarbeiterinnen und Mitarbeiter oder der Einführung grundlegen neuer Arbeitsmethoden.

Naturgemäß hat die Freienvertretung ein Interesse daran, so viele (personenbezogene) Daten wie möglich über ihre Klientel zu erhalten, um deren Interessen optimal vertreten zu können. Allerdings sind das Persönlichkeitsrecht und das Recht auf Datenschutz der Betroffenen zu berücksichtigen. Inzwischen bin ich zweimal zu Fragen der Reichweite der Auskunftsansprüche der Freienvertretung zu personenbezogenen Daten von der HA Personal konsultiert worden. Zusammengefasst lässt sich folgendes sagen: Die Weitergabe von personenbezogenen Daten an die Freienvertretung kann über die im Statut ausdrücklich geregelten Fälle hinaus nur auf die Einwilligung der Betroffenen gestützt werden. Davon unberührt bleibt das Recht, zur Erfüllung der Aufgaben der Freienvertretung anonyme Statistiken zu fordern. Insoweit ist das Berliner Datenschutzgesetz nicht einschlägig.

IV. Datenschutz im Programmbereich

1. Smart-TV

Im 10. und 11. Tätigkeitsbericht hat Herr Dr. Bismark bereits ausführlich zur Diskussion der Datenschutzaspekte im Zusammenhang mit der Nutzung von Smart-TV berichtet. Smart-TV bietet neben dem Fernsehempfang die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, sich simultan zum laufenden TV-Programm etwa durch den HbbTV-Standard über das Internet weitere Informationen wie zum Beispiel Programminformationen mit Trailern, Nachrichten oder Hinweise auf Sendungen aus den Mediatheken der Sender auf dem Bildschirm anzeigen zu lassen. Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender. Im Mai 2014 haben die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten gemeinsam mit den Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich ein gemeinsames Positionspapier zu Datenschutzfragen bei Smart-TV veröffentlicht (Anlage). 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.

Ende letzten Jahres haben der Datenschutzbeauftragte des Mitteldeutschen Rundfunks und ich gemeinsam 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. Die ARD hat damit in dieser Hinsicht deutschlandweit eine Vorreiterrolle eingenommen. In den überarbeiteten Datenschutzhinweisen wird allerdings auch klargestellt, dass es zur Bereitstellung der HbbTV-Angebote über das Internet technisch unerlässlich ist, die IP-Adresse des Zuschauers auf den Webserver zu übertragen. Wer dies nicht wünscht, muss auf die Verbindung zum Internet verzichten und das Fernsehgerät vom Internet trennen bzw. die Internetfunktionalität des Gerätes ausschalten.

2. Datenschutz bei der Online-Nutzungsmessung

Bereits im Herbst 2013 hat der **rbb** – wie auch einige andere ARD-Anstalten - einen Vertrag mit der Fa. AT Internet über Online-Nutzungsmessung abgeschlossen. Zwar war ich im Vorfeld über die beabsichtigte Zusammenarbeit informiert worden. Krankheitsbedingt war es mir dann allerdings nicht möglich, den endgültigen Vertragsentwurf hinsichtlich der datenschutzrechtlichen Implikationen zu prüfen. Erst im Herbst 2014 erfuhr ich von dem Vertragsschluss und bat nach Prüfung der Dokumente, die Vereinbarung zur Auftragsdatenverarbeitung mit der Firma zu optimieren. Das ist inzwischen geschehen. In der Fassung vom März 2015 ist nun dokumentiert, dass lediglich eine anonyme Auswertung des Nutzungsverhaltens unter Verwendung einer gekürzten IP-Adresse stattfindet. Die Datensicherheit ist durch ein überzeugendes Datensicherheitskonzept der Firma gewährleistet.

3. Neue Sportdatenbank

Im Frühjahr 2015 ist für die Bereiche **rbb**-text und ARD-Text eine neue Sportdatenbank eingeführt worden. Dabei handelt es sich um eine Software-Anwendung, die in Bedienung, Aussehen und Funktionalität weitgehend der alten Sportdatenbank entspricht.

Die in der Sportdatenbank verarbeiteten journalistischen Daten unterliegen dem Medienprivileg. Sie bedürfen zu ihrer Verarbeitung keiner speziellen Rechtsgrundlage. Zur Authentifizierung der Benutzer werden die Login-Eingaben gegen das entsprechende Benutzer-Passwort Tupel des Active Directory geprüft. Weitere Daten werden aus dem Active Directory weder gelesen noch ins Active Directory geschrieben.

Auf der Basis des vom Informationssicherheitsbeauftragten geprüften IT-Sicherheitskonzepts habe ich der Einführung der neuen Sportdatenbank zugestimmt.

4. Radioplayer für die ARD-Radiosender

Im Frühjahr 2015 hat die ARD beschlossen, dass die Hörfunkwellen der ARD mit dem Portal Radioplayer in das Internet getragen werden und die linearen Angebote auf diese Weise eine breitere Nutzung gerade beim jungen Publikum und bei den mobilen Ausspielwegen erfahren sollen. Auf diese Weise wird den Hörern angeboten, die Radio-Sender/Webstreams stationär oder mobil auf ihren Computern, Smartphones, Tablets etc. via Internet zu empfangen. Ursprünglich kommt das Verfahren von der BBC, die zusammen mit zwei großen privaten Radiostationen den Radioplayer uk gegründet hat.

Inzwischen hat die ARD einen Nutzungsvertrag mit Radioplayer.de zunächst für ein Jahr abgeschlossen. Die Verhandlungsführung lag bei WDR, HR und NDR. Neben den anderen ARD-Hörfunkprogrammen sind nun auch die **rbb**-Radioprogramme über das Portal abrufbar.

Zwar sieht die technische Infrastruktur, mit der Radioplayer arbeitet, die Verwendung von google analytics vor, um den Rundfunkanstalten entsprechende Auswertungen zur Verfügung stellen zu können. Allerdings arbeitet google analytics hier mit einer Anonymisierungsfunktion. Mit dieser Funktion hatte Google im Jahr 2011 auf die Kritik der deutschen Datenschützer reagiert. Die Radioplayer GmbH hat der ARD zugesichert, dass die Anonymisierung der IP-Adresse bei der Erfassung auf europäischen Servern erfolgt. So wird die IP-Adresse des Besuchers ohne Personenbeziehbarkeit nur noch in einer verkürzten Form an Google übermittelt. Die Aktivitäten der Hörer sind damit anonym und lassen sich nicht mehr zurückverfolgen. Die erhobenen Daten werden auch nicht mit anderen Daten wie demografischen Merkmalen oder Interessen verknüpft. Diese Funktionen von Google Analytics und alle Datenfreigabeeinstellungen sind bei Radioplayer deaktiviert.

Die User haben außerdem die Möglichkeit, der Übermittlung der Daten insgesamt zu widersprechen. Radioplayer hat sich ferner gegenüber der ARD verpflichtet, von seinen Kontrollrechten gegenüber Google regelmäßig Gebrauch zu machen und den ARD-Datenschutzbeauftragten die diesbezüglichen Berichte zur Verfügung zu stellen.

5. Einsatz von Drohnen bei der Fernsehproduktion

Im Juli 2014 habe ich mich mit dem Einsatz von Drohnen/Coptern im Rahmen von Fernsehproduktionen beschäftigt. Die Drohnen sind eine Ergänzung zur Krankamera, zur Hubschrauberkamera und z. B. zu Kameraaufnahmen vom Motorrad aus. Der wesentliche Unterschied zu den bisherigen Kameras besteht darin, dass Drohnen sehr schnell und kostengünstig zum Einsatz gebracht werden können. Da der **rbb** nicht selbst im Besitz derartiger Geräte ist, beauftragt er regelmäßig gewerbliche Anbieter mit der Herstellung von mit Drohnen hergestellten Aufnahmen. Während der Einsatz von Drohnen zu Sport- und Freizeitzwecken – sofern eine bestimmte Größe nicht überschritten wird – genehmigungs- und anzeigefrei ist, ist der Einsatz zu gewerblichen Nutzungszwecken erlaubnispflichtig. Die Geräte dürfen

nicht außerhalb der Sichtweite des Operators betrieben werden und nicht mehr als 25 kg wiegen.
Da die Aufnahmen mit Drohnen im Rahmen von Fernsehproduktionen unter das Medienprivileg fallen, unterliegen sie nicht dem strengen datenschutzrechtlichen Regelungswerk. Den entsprechenden Programmbereichen habe ich deutlich gemacht, dass bei den Aufnahmen mit Drohnen – wie üblich - darauf zu achten ist, dass die Persönlichkeitsrechte (insbesondere das Recht am eigenen Bild) etwaiger Passanten nicht verletzt werden. Das bedeutet, dass Großaufnahmen von Passanten ohne deren Einwilligung in der Regel nicht gestattet sind. Ausnahmen sind in Abstimmung mit dem Justitiariat zu klären.

V. Informationsmaßnahmen

Meine Informations- und Schulungsaufgabe habe ich im Berichtszeitraum wahrgenommen, indem ich zahlreiche Unterweisungen zu Datenschutz bei SAP durchgeführt habe und in verschiedenen hausinternen Besprechungen auf aktuelle und für den jeweiligen Aufgabenbereich relevante Fragen des Datenschutzes eingegangen bin.

Am 21. August 2014 habe ich erstmals zusammen mit dem Leiter des Bereichs Organisation und IT, Herrn Kruithof, das jährliche Datenschutzseminar für die neuen Auszubildenden beim **rbb** durchgeführt.

D. Datenschutz bei der Rundfunkteilnehmerdatenverarbeitung

I. Datenschutz beim Zentralen Beitragsservice

1. Allgemeines

Von 1976 bis 2012 hat die Gebühreneinzugszentrale (GEZ) die Rundfunkgebühren für die Landesrundfunkanstalten eingezogen. Mit der Umstellung auf das Beitragsfinanzierungssystem zum 1. Januar 2013 wurde aus der GEZ der Zentrale Beitragsservice.

Für den **rbb** ist auch beim Rundfunkbeitragseinzug das Berliner Datenschutzgesetz zu beachten (§ 36 Abs. 1 rbb-Staatsvertrag). Das Berliner Datenschutzgesetz ist auch auf die Verarbeitung der Beitragszahlerdaten beim Zentralen Beitragsservice anzuwenden, soweit es um Beitragszahler aus dem Sendegebiet des **rbb** geht. Vorrangig vor den allgemeinen Datenschutzgesetzen gelten für den Beitragseinzug die bereichsspezifischen Datenschutzregelungen des Rundfunkbeitragsstaatsvertrages (RBStV).

Die Überwachung des Datenschutzes bei der Verarbeitung der Rundfunkteilnehmerdaten obliegt dem Beauftragten für den Datenschutz des Landes Berlin im Benehmen mit dem oder der Landesbeauftragten des Datenschutzes des anderen Landes (§ 38 Abs. 8 **rbb**-Staatsvertrag). Als behördliche Datenschutzbeauftragte gemäß § 19 a BerlDSG bin ich für die ordnungsgemäße Datenverarbeitung beim **rbb** unmittelbar zuständig.

Unbeschadet der Zuständigkeit des nach Landesrecht für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ist beim Zentralen Beitragsservice gemäß § 11 Abs. 2 Satz 1 RBStV eine behördliche Datenschutzbeauftragte bestellt. Gemäß den Regelungen des § 11 Abs. 2 RBStV arbeitet die behördliche Datenschutzbeauftragte des Beitragsservices 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 den behördlichen Datenschutzbeauftragten anwendbaren Bestimmungen des Bundesdatenschutzgesetzes entsprechend. Die behördliche Datenschutzbeauftragte übt diese Aufgabe neben ihrer Tätigkeit als Leiterin der Abteilung Zentrale Aufgaben beim Zentralen Beitragsservice aus. Seit 1. Juni 2006 wird sie durch eine Vollzeitkraft bei der Wahrnehmung ihrer Datenschutzaufgaben unterstützt.

2. Auskunftsersuchen und Eingaben

Die Datenschutzbeauftragten der Rundfunkanstalten haben die Bearbeitung und Beantwortung von Anfragen und sonstigem Routineschriftwechsel in Datenschutzangelegenheiten dem Zentralen Beitragsservice übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter und von individuellen Anfragen mit besonderer datenschutzrechtlicher Bedeutung haben sie sich selbst vorbehalten.

Im Jahr 2014 hat die Datenschutzbeauftragte des Zentralen Beitragsservices folgende Vorgänge aus dem Sendegebiet des **rbb** für mich bearbeitet:

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

Ich selbst habe in 2014 folgende Vorgänge bearbeitet:

Ersuchen von Bürgerinnen und Bürgern um Auskunft über zu ihrer Person gespeicherte Daten:	12

Fragen zur Beauftragung der **rbb** media im nicht-privaten Bereich:	1
Fragen zur Berechtigung der Datenverarbeitung:	4
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz:	7
Anzahl der Vorgänge insgesamt:	**24**

3. Auslagerung des Druckbereichs beim Zentralen Beitragsservice

Im Frühjahr 2014 hatte der Zentrale Beitragsservice die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio konsultiert und nach den Möglichkeiten und Grenzen der Auftragsdatenverarbeitung und des Outsourcings gefragt. Konkret ging es um die Zulässigkeit der bereits bestehenden Auslagerung des Druckbereichs.

Wir haben bestätigt, dass eine Outsourcing-Lösung im Druckbereich zulässig ist. Im Juni 2014 erfolgte eine Prüfung des aktuellen Druckdienstleisters, an der neben der Datenschutzbeauftragte und des Revisionsleiters des Beitragsservices auch der Datenschutzbeauftragte des NDR teilnahm. Die Prüfung ergab keine Beanstandungen.

II. Datenschutz beim rbb-Beitragsservice

Bei Fragen zum Datenschutz im Zusammenhang mit dem Beitragseinzug ist neben der behördlichen Datenschutzbeauftragten des Zentralen Beitragsservice und ihrem Mitarbeiter auch der Leiter des **rbb**-Beitragsservices ein wichtiger Ansprechpartner. Während sich die Zusammenarbeit mit der Kollegin beim Zentralen Beitragsservice auf die Sicherstellung der Einhaltung des Datenschutzes bei dem dort abzuwickelnden Massenverfahren und auf die Beantwortung einzelner Datenschutzbeschwerden konzentriert, werde ich vom Leiter des **rbb**-Beitragsservices hauptsächlich in datenschutzrechtlichen Fragen bezüglich der datenschutzkonformen Organisation der Arbeit vor Ort konsultiert.

1. Vertrag mit der wdr mediagroup zur Bestandspflege im nicht-privaten Bereich

Wie in meinen früheren Tätigkeitsberichten erwähnt, hatte der **rbb** im Zusammenhang mit der Umstellung auf das Beitragsfinanzierungssystem Anfang 2013 seine 100%ige Tochter **rbb** media damit beauftragt, die telefonische Klärung beitragsrelevanter Daten im nichtprivaten Bereich vorzunehmen. Mit Wirkung zum 1. März 2015 ist die telefonische Beratung von nichtprivaten Rundfunkteilnehmerinnen und –teilnehmern für den **rbb** von der **rbb** media auf die wdr mediagroup übergegangen. Die vertraglichen Vereinbarungen einschließlich der Vereinbarung über Auftragsdatenverarbeitung entsprechen im Wesentlichen denjenigen Vereinbarungen, die der **rbb** mit der **rbb** media getroffen hatte. Die Mitarbeiter der wdr mediagroup wurden vor Aufnahme ihrer Tätigkeit u.a. zum Datenschutz unterwiesen.

Zu der Arbeit der wdr mediagroup hat mich bislang keine Beschwerde erreicht.

2. Inboundtelefonie

Im Frühjahr 2014 ist zur effizienten Bearbeitung eingehender Telefonate von (potentiellen) Beitragszahlern eine einheitliche Servicenummer für die Landesrundfunkanstalten – 0185 999 555 – etabliert worden. Alle Anrufer auf dieser Rufnummer werden zunächst in den 1st-Level des zentralen Beitragsservices geleitet und von dort bei Bedarf an die zuständige Landesrundfunkanstalt weitergeleitet. Mit dieser Bündelung der Anrufe soll eine einheitliche Sprachregelung für die Kommunikation des Rundfunkbeitrages gewährleistet und Kostenersparnisse realisiert werden.

Als Basis dient die bestehende Telefoninfrastruktur des Zentralen Beitragsservices. Die Verteilung der Anrufe erfolgt mittels einer speziellen Software in einem internetbasierten Netzwerk. Das Routing erfolgt in Kombination Daten/Sprache. Das bedeutet, dass das Signaling zwar über Daten erfolgt, jedoch das gesprochene Wort weiterhin per Telefon (ISDN) übertragen wird. Die sog. Voice-over-IP (VOiP)-Variante wurde ganz bewusst nicht eingesetzt. Somit ist ein Abhören im Datenver-

kehr nicht möglich. Die Benutzerinnen und Benutzer im **rbb**-Beitragsservice müssen sich jeweils im System einloggen, damit ihnen Anrufe von Köln aus zugeleitet werden können. Sie benötigen für die Anmeldung am System eine Internetanmeldung, einen Benutzernamen, ein Passwort und eine Telefonnummer bzw. Durchwahl des aktuellen Arbeitsplatzes.

Vor dem Hintergrund, dass eine personenbezogene Auswertung der Telefonate schon aufgrund der inzwischen nur noch sehr wenigen pro Tag an den **rbb**-Beitragsservice durchgestellten Anrufe überhaupt nicht möglich ist, konnte ich dem Regelbetrieb zustimmen.

3. Wunsch der Vollstreckungsbehörden nach Kennzeichnung der sog. direkt angemeldeten Bürgerinnen und Bürger

Ende 2014 fragte der Leiter des Beitragsservices an, ob gegenüber den Vollstreckungsbehörden im Zusammenhang mit Vollstreckungsersuchen durch ein zusätzliches Kennzeichen angezeigt werden könne, ob es sich um langjährige und säumige Rundfunkgebührenschuldner oder um auf der Basis der übermittelten EMA-Daten neu angemeldete Personen handele. Diese zusätzliche Information hatten die Vollstreckungsbehörden zur besseren Vorbereitung auf etwaige Einwendungen der Vollstreckungsschuldner erbeten.

Ich habe geantwortet, dass es für die Übermittlung dieses Merkmals keine Rechtsgrundlage gibt. Aus diesem Grund musste darauf verzichtet werden.

E. 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 IT-Sicherheitsbeauftragten in allen datenschutzrechtlich relevanten Fragen und Vorgängen einbezogen.

1. Geänderte Verwaltungsvereinbarung ab 1.1.2015

In ihrer Sitzung vom 25. November 2013 haben die Intendantinnen und Intendanten beschlossen, dass künftig einzelne gemeinschaftlich betriebene Einrichtungen der Gremienkontrolle der jeweiligen Sitzanstalt unterliegen. Aus diesem Grund ist die Zustimmungspflicht des **rbb**-Verwaltungsrats für bestimmte Rechtsgeschäfte in die Verwaltungsvereinbarung aufgenommen worden. Neben weiteren Änderungen zur Wirtschaftsführung wurde die Verwaltungsvereinbarung auf Anregung der Datenschutzbeauftragten und der Informationssicherheitsbeauftragten des IVZ um die Themen Datenschutz und Datensicherheit ergänzt. Danach ist die Geschäftsführung des IVZ verpflichtet, sich mit den Datenschutzbeauftragten und IT-Sicherheitsbeauftragten regelmäßig über Projekte mit Relevanz für den Datenschutz und die Informationssicherheit abzustimmen und über datenschutzrechtlich relevante Vorgänge unverzüglich zu informieren. Auch die Pflicht zur Bestellung einer/eines Informationssicherheitsbeauftragten, zur Betreibung eines Informationssicherheits-Managementsystems und zur Einführung eines standardisierten Verfahrens des Risikomanagements wurde in der Verwaltungsvereinbarung verankert.

2. Fehlerhafter Versand von Honorarabrechnungen

Im Oktober 2014 kam es aufgrund eines technischen Defekts an der Kuvertiermaschine, die beim Versand der Honorarabrechnungen des **rbb** im IVZ eingesetzt wird, zu einem fehlerhaften Versand von zahlreichen Honorarabrechnungen. Bis zu 700 freie Mitarbeiterinnen und Mitarbeiter haben Honorarabrechnungen bzw. Teile von Honorarabrechnungen anderer Mitarbeiterinnen und Mitarbeiter erhalten, die nicht für sie bestimmt waren.

Unmittelbar nach Kenntnis des technischen Fehlers hat mich die HA Personal informiert. HA Personal und ich haben gemeinsam entschieden, alle möglicherweise betroffenen Kolleginnen und Kollegen anzuschreiben und über den fehlerhaften Versand zu informieren. Bei einer Besprechung mit dem Geschäftsführer und mehreren Mitarbeitern in den Räumlichkeiten des IVZ, an dem auch der stellvertretende Personalleiter teilnahm, wurde der Ursache des Fehlers weiter auf den Grund gegangen. Danach war der fehlerhafte Versand durch eine außerplanmäßige Beilage hervorgerufen, durch die sich die Anzahl der Blätter pro Brief verändert hatte. Es wurde noch einmal klargestellt, dass das IVZ nach der Fehlerbehebung und nach jeder Änderung im Druckablauf befugt und verpflichtet ist, Stichproben der Abrechnungen zu öffnen und auf Plausibilität zu prüfen. Außerdem wurde dieser Vorfall zum Anlass genommen zu prüfen, ob eine Versendung der Gehalts- und Honorarabrechnungen in der Perspektive per Mail in Frage kommt. Für die Erarbeitung eines entsprechenden Konzepts wurde eine Arbeitsgruppe ins Leben gerufen, deren Mitglied ich bin.

3. Forensische Untersuchung von Festplatten

Anfang 2015 war aufgrund eines Schadsoftware-Alarms und einer ersten Prüfung der Virenscanner-Logs auf zwei Laptops des IVZ am Standort Köln der Anfangsverdacht gegeben, dass die beiden Rechner nicht gemäß der Sicherheitsregeln von den IVZ-Mitarbeitern genutzt wurde. Aus diesem Grund wurde in enger Abstimmung mit der HA Personal und mir auf der Grundlage der einschlägigen IVZ-internen Regelungen und mit Wissen der Betroffenen eine interne forensische Untersuchung der Laptops durchgeführt. Hierfür wurden die Festplatten ausgebaut und versiegelt an den Standort Berlin gebracht. Dort wurden sie von der Informationssicherheitsbeauftragten auf verbotene Software und Daten – auch gelöschte Daten – untersucht. Die Liste der Funde hat in dem einem Fall den Anfangsverdacht bestätigt und zu einer arbeitsrechtlichen Abmahnung geführt, in dem anderen Fall war kein gravierender Verstoß gegen die Sicherheitsvorgaben festzustellen.

Ich war während der gesamten Untersuchung, also seit der Öffnung der versiegelten Transporttaschen, anwesend.

4. Jährliches Treffen der Datenschutzbeauftragten

Am 25. November 2014 fand beim IVZ das jährliche Treffen der Datenschutzbeauftragten der beteiligten Anstalten statt. Der Geschäftsführer, Herr Dr. Greten, stellte den neuen Leiter des Rechenzentrums Berlin und den neuen stellvertretenden Informationssicherheitsbeauftragten des IVZ vor. Herr Dr. Greten berichtete über die Übernahme des Hostings der IT-Infrastruktur der Baden-Badener Pensionskasse von einem externen Rechenzentrum zum 1. Juli 2014 Die IT- Sicherheitsbeauftragte präsentierte die Vorgehensweise des IVZ beim Risikomanagement.

5. ARD Box

Cloud Computing ist das dynamisch an den Bedarf angepasste Anbieten und Nutzen von IT-Dienstleistungen - insbesondere Speicherkapazitäten - über ein Netz. Durch die einfache, schnelle und flexible Nutzung wird Cloud Computing auch vermehrt in den Rundfunkanstalten angewendet. Einsatzfelder einer Cloud im öffentlich-rechtlichen Rundfunk sind u.a. die Produktion, die Planung und die Recherche.

Bei der Nutzung einer öffentlichen Cloud besteht die Gefahr darin, dass die Nutzer in der Regel keinen vollständigen Einfluss auf den Standort und die Sicherheitsvorkehrungen der Cloud ausüben können. Aus diesem Grund lehnen wir Datenschützer von ARD, ZDF und DLR die Nutzung von öffentlichen Clouds – jedenfalls für Daten mit mittlerem bis hohem Schutzbedarf - ab.

Das IVZ bietet nun als Alternative ab Anfang 2016 allen ARD-Anstalten die Nutzung der ARD Box an. Diese unternehmenseigene Cloud stellt einen ortsunabhängigen Speicherbereich für Daten zur Verfügung und ist aus dem Internet erreichbar. 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.

Gemeinsam mit dem Mitarbeiter der Datenschutzbeauftragten des WDR habe ich die Nutzungsbedingungen und die Datenschutzerklärung der ARD Box erarbeitet. Derzeit befindet sich die ARD-Box in einer Testphase.

Dabei ist Folgendes aufgefallen: Zwar findet zwischen Client und IVZ-Server eine SSL-Verschlüsselung statt. Jedoch existiert keine lokale Verschlüsselung von Kundendaten auf den Servern.

Deshalb habe ich empfohlen, Dokumente mit einem erhöhten Schutzbedarf - wenn überhaupt - nur als verschlüsselte Datei in der ARD Box zu laden. Investigative Bereiche sollten auf die Nutzung auch dieser Cloud verzichten.

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 Jahr 2014 fanden zwei reguläre Sitzungen des AK DSB statt, und zwar am 2./4. April beim BR in München und am 25./26. September bei der Deutschen Welle in Bonn.

Bei der Frühjahrssitzung, auf der mich Herr Dr. Bismark vertreten hat, standen unter anderem das Gesetzgebungsverfahren zur EU-Grundschutzverordnung, die Möglichkeiten und Grenzen der Auftragsdatenverarbeitung und des Outsourcing beim Zentralen Beitragsservice auf der Agenda.

Auf unserer Herbst-Sitzung haben wir uns u. a. eingehend mit der Evaluierung des Rundfunkbeitragsstaatsvertrages beschäftigt. Zu diesem Tagesordnungspunkt nahm der Justitiar des SWR, Herr Dr. Eicher, als Gast teil. Ein Thema war dabei die Notwendigkeit eines wiederholten Komplett-Meldedatenabgleichs. Im Unterschied zum Ankauf von Adressdaten liefere der Meldedatenabgleich seriöse und weitgehend zutreffende Daten. Herr Dr. Eicher erläuterte auch, dass der kontinuierliche Meldedatenabgleich nicht sämtliche Konstellationen abdecke. So sei etwa der Wegzug eines Beitragszahlers aus einer gemeinsamen Wohnung oder die Beitragssituation nach dem Tode eines von mehreren Wohnungspartners hierdurch nicht zu erfassen. Ein weiteres Thema war die Frage der Notwendigkeit der Verarbeitung weiterer Kommunikationsdaten wie Telefon und E-Mail. Außerdem ging es um die Übernahme der Satzungsvorschriften zum Datenschutz in den Rundfunkbeitragsstaatsvertrag.

Eingehend haben wir uns auch mit dem Urteil des Europäischen Gerichtshofs zu Google befasst. Wir waren uns darin einig, dass das Urteil für die Rundfunkanstalten als sehr hilfreich anzusehen ist. Das Gericht hat konstatiert, dass aufgrund des datenschutzrechtlichen Medienprivilegs die Medien selbst zur Löschung nicht verpflichtet sind. Dieses Privileg, so der EuGH ausdrücklich, stehe den Suchmaschinenbetreibern nicht zu. Darin ist eine Stärkung der klassischen Medien zu sehen.

Das Schwerpunktthema der Sitzung war der Datenschutz bei der Online-Nutzungsmessung.

Der Geschäftsführer der Firma INFOnline stellte im Rahmen einer Präsentation das SZM-Messverfahren vor, das neben anderen Messverfahren bei den meisten Rundfunkanstalten hinsichtlich ihrer Online-Angebote und auch bei den HbbTV-Angeboten zum Einsatz kommt. Im Jahr 2011 hatte INFOnline mit den Landesdatenschutzbeauftragten die Umsetzung folgender Maßnahmen vereinbart:

- Kürzung der IP-Adresse um 8 Bit vor jeglicher Verarbeitung,
- Einführung einer „Opt-out-Funktion und

- Bereitstellung einer Vereinbarung zur Auftragsdatenverarbeitung für alle SMZ-Kunden durch INFOnline.

Der Hessische Rundfunk hat für die ARD-Anstalten federführend eine derartige Vereinbarung zur Auftragsdatenverarbeitung geschlossen. Darüber hinaus hat die Unterarbeitsgruppe „Beitragseinzug", der ich angehöre, am 11. Juni 2014 eine Telefonkonferenz durchgeführt, und zwar zum Thema „Telefonnummern im Beitragseinzug".
Außerdem habe ich zusammen mit einigen anderen Vertretern des AK DSB zudem an einem Gespräch mit den Rundfunkreferenten, den Rundfunkanstalten und mit einigen Landesdatenschutzbeauftragten teilgenommen, das dem Thema „Evaluierung des Rundfunkbeitragsstaatsvertrages" gewidmet war und am 21. Oktober 2014 in Berlin stattgefunden hat (s. S. 21 ff.).

II. Arbeitskreis Medien der Datenschutzbeauftragten von Bund und Ländern

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

Im Berichtszeitraum habe ich den AK DSB auf der Sitzung des AK Medien am 25. Februar 2015 vertreten. Themen waren unter anderem die Datenschutzanforderungen bei HbbTV-/Smart-TV-Endgeräten und die Evaluation des Rundfunkbeitragsstaatsvertrages – hier insbesondere die Frage der Notwendigkeit der Durchführung eines weiteren kompletten Meldedatenabgleichs. Außerdem habe ich aus dem Arbeitskreis der Rundfunkdatenschutzbeauftragten berichtet. Dabei fanden angeregte Diskussionen zur "Google-Entscheidung", zum Einsatz von Drohnen für Filmaufnahmen und zur Online-Nutzungsmessung statt.

III. Teilnahme an Fortbildungen und Veranstaltungen

Am 22./23. Mai 2014 habe ich an dem @kit-Kongress „Datenschutz und Datensicherheit als Herausforderung des Rechts“ in Berlin teilgenommen. Das gab mir nach meinem längeren krankheitsbedingten Ausfall einen guten Überblick über die auf europäischer und bundesdeutscher Ebene diskutierten Themen. Auf der Agenda standen u. a. eine öffentliche Podiumsdiskussion zum Thema „Datenschutz und Datensicherheit nach dem NSA-Skandal“, Vorträge zu Datenschutz in der Cloud und Datenschutz bei mobilen Endgeräten sowie Panel zu Big Data und zum Stand der Europäischen Datenschutzreform.

Am 3./ 4. Juni 2014 habe ich an einem Symposium des Instituts für Rundfunktechnik zum Thema „Cloud Computing im Rundfunk“ beim ZDF in Mainz teilgenommen. Cloud Computing ist das dynamisch an den Bedarf angepasste Anbieten und Nutzen von IT-Dienstleistungen über ein Netz. Zu unterscheiden ist die sog. Private von der Public Cloud. Während die Private Cloud eine unternehmenseigene und von diesem Unternehmen selbst betriebene Cloud-Umgebung ist, ist das Public Cloud-Angebot ein öffentlich verfügbares Cloud-Serviceangebot, das über das Internet angeboten wird. Hier werden die IT-Infrastruktur, die Cloud-Serviceangebote sowie der IT-Betrieb vom Anbieter gestellt und durchgeführt. Durch die genutzte Technik ist es möglich, die IT-Leistung dynamisch über mehrere Standorte zu verteilen, die geografisch weit verstreut sein können, z. B. im Inland und auch im Ausland. Dadurch besteht nur eine eingeschränkte bzw. keine Kontrollmöglichkeit auf die Sicherheit der ausgelagerten Prozesse, Anwendungen und Daten. Eine Zwischenlösung bietet die Community Cloud. In einer Community Cloud schließen sich unterschiedliche Organisationen zu einer Community zusammen und bilden aus ihren Private Clouds eine Community Cloud. Dabei wird versucht, bei vergleichbaren Aufgaben, Vorgaben oder Sicherheitsanforderungen die vorhandenen Infrastrukturen gemeinsam zu nutzen. Ein Beispiel für eine Community Cloud ist das Cloud-Angebot des IVZ.

Durch die einfache, schnelle und flexible Nutzung wird Cloud Computing auch vermehrt in den Rundfunkanstalten angewendet. Mögliche Einsatzfelder einer Cloud im

öffentlich-rechtlichen Rundfunk, z. B. in der Produktion, bei der Planung, Recherche und Publikation, wurden auf dem Symposium ausführlich erörtert. Ausführlich wurde aber auch auf die rechtlichen Rahmenbedingungen und Risiken eingegangen. Bei der Public Cloud sind die Anforderungen an die Auftragsdatenverarbeitung einzuhalten.

Die Frage, ob die Nutzung einer Public Cloud überhaupt in Frage kommt, hängt vom Schutzbedarf der zu verarbeitenden Daten ab. Bei hohem Schutzbedarf scheidet die Public Cloud von vornherein aus. Ansonsten sollten abhängig vom Schutzbedarf und der Cloud-Organisationsform die IT-Infrastruktur sowie die benutzten Anwendungen mindestens denselben IT-Sicherheitsstandard aufweisen wie in der eigenen IT-Umgebung. Dies ist durch entsprechende vertragliche Vereinbarungen sicherzustellen.

Am 3. Februar 2015 habe ich an einem Fachseminar für Datenschutzbeauftragte zum Thema „Mitarbeiter im Datenschutz richtig schulen" teilgenommen. Schwerpunkte des Seminars waren die richtige Konzeption und der Methodenmix effektiver Schulungen. Für mich besonders interessant war die Einheit zum Methodenmix. Die jeweiligen Vorzüge von sog. Web Based Trainings und von Präsenzschulungen wurden herausgearbeitet. Um den hohen Bedarf an Datenschutz-Schulungen und –Unterweisungen im **rbb** abzudecken, beabsichtige ich, zukünftig das Web Based Training einzusetzen, um zumindest den Mitarbeiterinnen und Mitarbeitern erste Grundlagen zu vermitteln. Den Mitarbeiterinnen und Mitarbeiter werden online bestimmte Informationen zum Thema gegeben. Der Vorteil ist, dass die Mitarbeiterinnen und Mitarbeiter Zeitpunkt und Geschwindigkeit des Trainings selber für sich festlegen können. Dazu bin ich mit der HA Personal, die für die Organisation von Schulungen und hausinternen Fachseminaren im **rbb** grundsätzlich zuständig ist, und mit dem Bereich OuI im Gespräch. Möglicherweise bietet es sich an, künftig auch andere Themen auf diese Art im **rbb** zu vermitteln.

Berlin, 14.8.2015

gez. Anke Naujock

Anlagen

Stellungnahme des AK DSB im Rahmen der Evaluations zu den Datenschutzbestimmungen im Rundfunkbeitragsstaatsvertrag (RBStV) vom 30. Januar 2015

Gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit Datenschutz“ vom Mai 2014