9. Tätigkeitsbericht

der Beauftragten für den Datenschutz

des

Rundfunk Berlin-Brandenburg

Berichtszeitraum:

01. April 2011 bis 31. März 2012

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

Inhaltsverzeichnis

Vorbemerkung

Am 16. Dezember 2011 hat Schleswig-Holstein als letztes Bundesland den Rundfunkbeitragsstaatsvertrag ratifiziert, der – bis auf die bereits seit 1. Januar 2012 geltenden Übergangsvorschriften - in seinen wesentlichen Teilen zum 1. Januar 2013 in Kraft treten wird. In diesem Zusammenhang waren und sind auch die Rundfunkdatenschutzbeauftragten ganz besonders gefordert. Vom Beginn des Gesetzgebungsverfahrens an bis zur Ratifizierung haben wir den Prozess mit unseren datenschutzrechtlichen Stellungnahmen begleitet. Dies setzt sich nunmehr bei der Erarbeitung der Rundfunkbeitragssatzung fort. Außerdem stehen wir der Abteilung Rundfunkgebühren und der GEZ bei datenschutzrechtlich relevanten Fragen im Zusammenhang mit der Umstellung auf das Beitragssystem und bei der Auslegung der zukünftigen datenschutzrechtlich relevanten Bestimmungen zur Seite. Ich gehe davon aus, dass das Thema „Datenschutz beim Rundfunkgebühren- bzw. –beitragseinzug“ auch in der Umsetzungsphase ab 2013 und in der gesamten Evaluierungsphase bis 2015 noch einen Schwerpunkt meiner Tätigkeit bilden wird.

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

Meiner Kollegin im Sekretariat, Frau Ruthild Just, dem stellvertretenden behördlichen Datenschutzbeauftragten, Herrn Dr. Bismark, und dem IT-Sicherheitsbeauftragten, Herrn Wolff, 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 in aller Regel 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 § 38 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 §38 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 (§38 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 Leiters der Revision, Herrn Dr. Bismark, als stellvertretendem behördlichen Datenschutzbeauftragten hat die Intendantin entsprechend verlängert. Herr Dr. Bismark 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.

Für die Datensicherheit im **rbb** ist der Systemverantwortliche für IT-Sicherheit, 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 Rundfunkgebühreneinzug.

B. Entwicklung des Datenschutzrechts

I. Europa

1. Novellierung des EU-Datenschutzrechts

Am 25. Januar 2012 hat die Europäische Kommission ihre Vorschläge für eine umfassende Reform des EU-Datenschutzrechts veröffentlicht.

Im Fokus steht der Entwurf der Datenschutz-Grundverordnung. Da die Datenschutz-Grundverordnung auch auf den Datenschutz im Medienbereich eingeht, wären die Rundfunkanstalten unmittelbar von der Neuregelung betroffen.

Auch die derzeit gültige EU-Datenschutzrichtlinie umfasst schon den Datenschutz im Medienbereich. Allerdings wirken Europäische Richtlinien im Unterschied zu Verordnungen nicht unmittelbar, sondern bedürfen einer Umsetzung in den nationalstaatlichen Gesetzen. In den Deutschen Datenschutzgesetzen konnte auf diese Weise den Besonderheiten des Deutschen Rundfunksystems Rechnung getragen werden.

Nach Auffassung der Rundfunkdatenschutzbeauftragten muss der beim Mediendatenschutz erforderliche Prozess der Abwägung zwischen den Grundrechten auf Datenschutz einerseits und der Meinungsfreiheit andererseits in mitgliedstaatlicher Obhut bleiben. Deswegen wäre es folgerichtig – sollte es beim Instrument der Verordnung bleiben – eine Ausnahme für den Medienbereich zu formulieren. Auf jeden Fall aber müssen aus Sicht der Rundfunkanstalten noch Änderungen am Kommissionsentwurf mit dem Ziel vorgenommen werden, die Medienfreiheit weiter zu sichern.

Die Organisation der Datenschutzkontrolle und der entsprechenden Kontrollinstanzen ist ein wichtiger Aspekt der Medienfreiheit. Der/Die Datenschutzbeauftragte der Rundfunkanstalten muss weiterhin als Aufsichtsbehörde im Sinne der Verord-

nung gelten, zumal sich die Datenschutzkontrolle im öffentlich-rechtlichen Rundfunk als besonders effizient erwiesen hat. Die speziell ausgestaltete Datenschutzaufsicht, die auf der medienspezifischen Organisation und sachnahen Zugriffsmöglichkeit basiert, bewirkt eine besonders enge Kontrolldichte. Gleichwohl ist die Unabhängigkeit organisatorisch voll abgesichert.

Die Regelungen in der geplanten Verordnung zum Datenschutz bei Minderjährigen müssen optimiert werden. Bislang ist vorgesehen, dass bis zum vollendeten 13. Lebensjahr eines Kindes die Elterneinwilligung insbesondere zur Nutzung von Online-Angeboten erforderlich ist. Aus unserer Sicht ist der Entwurf nicht ausreichend flexibel für eine jugendschutzorientierte Handhabung des Datenschutzes (Stichwort: „Erziehung zur Datenschutz-Mündigkeit"). Die vorgesehene Altersgrenze von 13 Jahren ist zu starr: Für kommerzielle Angebote ist sie unter Umständen zu niedrig angelegt (und es sollte insoweit bei der Altersgrenze bei 18 Jahren bleiben), für kindgerechte Angebote ist sie gegebenenfalls zu hoch. Auf diese Weise würden Kinder aus am Wohl des Kindes orientierten und ausreichend geschützten Angeboten im Netz ausgeschlossen.

Unsere Standpunkte werden wir über das ARD-Verbindungsbüro in Brüssel in den Normgebungsprozess einbringen.

2. Klage der EU-Kommission gegen Deutschland vor dem Europäischen Gerichtshof

Wie in meinem letzten Tätigkeitsbericht erwähnt, hat das Bundesverfassungsgericht die deutschen Vorschriften zur Vorratsdatenspeicherung im „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" mit Urteil vom 2. März 2010 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 verstoße allerdings nicht generell gegen das Grundgesetz.

Die Regelungen gingen auf die Europäische Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von Daten zurück. Diese Richtlinie verpflichtet die Mitgliedstaaten der Europäischen Union, nationale Gesetze zu erlassen, nach denen bestimmte Daten, die bei der Bereitstellung und Nutzung öffentlicher elektronischer Kommunikationsdienste anfallen, von den Diensteanbietern auf Vorrat gespeichert werden müssen. Gespeichert werden sollen insbesondere Verkehrs- und Standortdaten. Inhaltsdaten – also Inhalte von E-Mails und Telefonaten – sollen nicht gespeichert werden.

Am 18. April 2011 hat die EU-Kommission ihren Bericht zur Evaluation der umstrittenen EU-Richtlinie zur Vorratsdatenspeicherung vorgelegt. Danach bestehen gravierende Mängel. Eine Überarbeitung der Richtlinie ist erforderlich. Trotz dieser Bewertung hat sie Deutschland inzwischen vor dem Europäischen Gerichtshof wegen Nichtumsetzung der Europäischen Richtlinie verklagt.

Die Innenminister der Länder und vor allem Unionspolitiker drängen mit zunehmender Schärfe auf eine Neuauflage der Vorratsdatenspeicherung. Weil die zuständige Justizministerin Leutheuser-Schnarrenberger die Daten aber nur wenige Tage speichern möchte und das Innenministerium auf einer längeren Speicherdauer besteht, gibt es in dem Streit keine Bewegung.

II. Bund

1. Beschäftigtendatenschutz

Am 28. Mai 2010 hat das Bundesinnenministerium einen Referentenentwurf für ein Gesetz zur Regelung des Beschäftigungsdatenschutzes vorgelegt. Nachdem dieser Entwurf aufgrund der Abstimmung zwischen den Bundesministerien stark verändert und erweitert worden war, hat ihn das Bundeskabinett am 25. August 2010

beschlossen. Am 5. November 2010 hat der Bundesrat dazu Stellung genommen. Am 25. Februar 2011 ist er in erster Lesung im Bundestag beraten und in die zuständigen Ausschüsse weiterverwiesen worden. Außerdem wurde ein eigener Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN zum Beschäftigtendatenschutz beraten. Am 18./19. Mai 2011 haben die Justizministerinnen und –minister der Länder auf ihrer Konferenz in Halle eine Ergänzung des Regierungsentwurfs gefordert. Unter anderem müssten die Arbeitgeber die Beschäftigten verpflichtend informieren, welche Daten erhoben und gespeichert werden. Darüber hinaus müssten anlasslose Screening-Verfahren ausgeschlossen werden. Bei einer öffentlichen Sachverständigenanhörung im Innenausschuss des Bundestages am 23. Mai 2011 wurde der Regierungsentwurf zum Beschäftigtendatenschutz kontrovers diskutiert. Zudem ging es in der Anhörung um Gesetzesentwürfe der SPD-Fraktion, der Fraktion BÜNDNIS 90/DIE GRÜNEN und der Fraktion Die Linke. Am 29. September 2011 hat der Bundestag einen Antrag der SPD-Fraktion zur Regelung des Beschäftigtendatenschutzgesetzes in einem eigenen Gesetz beraten und ihn in die zuständigen Ausschüsse verwiesen. Auf ihrer Herbstkonferenz in Berlin am 09. November 2011 haben die Justizministerinnen und Justizminister der Länder bekräftigt, dass eine umfassende Regelung des Beschäftigtendatenschutzes dringend erforderlich sei.
Es muss bezweifelt werden, ob noch in dieser Legislaturperiode ein Beschäftigtendatenschutzgesetz in Kraft treten wird.

2. ELENA

In meinem 7. Tätigkeitsbericht hatte ich darüber berichtet, dass am 28.03.2009 das sog. ELENA-Verfahrensgesetz beschlossen worden war. Das Gesetz war zum 1. Januar 2010 in Kraft getreten. ELENA sollte im Zusammenhang mit der Beantragung von Sozialleistungen die Arbeitgeber von der aufwändigen Erstellung einer Vielzahl von Bescheinigungen entlasten und gleichzeitig das Verfahren für die Antragsteller vereinfachen. Zu diesem Zweck waren die Arbeitgeber seit dem 1. Januar 2010 gesetzlich verpflichtet, monatlich eine entsprechende Meldung an eine bundesweit zentrale Speicherstelle zu versenden.

ELENA ist auf massive Kritik unter anderem der Datenschutzbeauftragten gestoßen. Auch die Personalräte von ADR, ZDF und Deutschlandradio hatten in einer gemeinsamen Erklärung vom 27. Januar 2010 gegen ELENA protestiert und eine Rücknahme des ELENA-Gesetzes gefordert.

Durch ein entsprechendes Aufhebungsgesetz, das am 3. Dezember 2011 in Kraft getreten ist, wurde das ELENA-Verfahren nun eingestellt und die gespeicherten Daten gelöscht.

Bereits in einer Presseerklärung vom 18. Juli 2011 hatte das Bundesministerium für Wirtschaft und Technologie seine Absicht bekannt gegeben, das ELENA-Verfahren schnellst möglich einzustellen. Als Grund dafür wurde die fehlende Verbreitung der qualifizierten elektronischen Signatur genannt, welche sich „trotz aller Bemühungen in absehbarer Zeit nicht flächendeckend verbreiten wird." Bereits unmittelbar nach Bekanntwerden dieser Absicht hat der **rbb** seine Datenzulieferung an die zentrale Stelle eingestellt.

3. Bundesmeldegesetz

Wie im letzten Tätigkeitsbericht erwähnt, ist das Meldewesen, das bislang Ländersache war, mit der Föderalismusreform I im Jahr 2006 in die ausschließliche Gesetzgebung des Bundes überführt worden. Seit Ende März 2011 liegt der Referentenentwurf eines Gesetzes zur Fortentwicklung des Meldewesens vor. Mit diesem Gesetz soll in Erfüllung der Gesetzgebungskompetenz des Bundes ein Bundesmeldegesetz geschaffen werden, das das bisher geltende Melderechtsrahmengesetz (MRRG) aus dem Jahre 1980 und die bisherigen Landesmeldegesetze ersetzt.

Die Rundfunkanstalten haben zu dem Entwurf Stellung genommen und gefordert, dass auch nach Inkrafttreten des Bundesmeldegesetzes die bisherige regelmäßige Meldedatenübermittlung bei Umzügen und auch die Einzel- und Gruppenauskünfte gegenüber den Rundfunkanstalten im Zusammenhang mit dem Rundfunkgebühren- bzw. -beitragseinzug weiter möglich sein müssen.

Das Gesetzgebungsverfahren dauert noch an. Bereits jetzt zeichnet sich allerdings ab, dass mit einem Inkrafttreten des Bundesmeldegesetzes (BMeldG) frühestens zum 1. Januar 2015 zu rechnen ist. Damit wird der in § 14 Abs. 9 Rundfunkbeitragsstaatsvertrag geregelte einmalige Meldedatenabgleich zum Zwecke der Bestands- und Ersterfassung der Beitragszahler, der zwischen dem 01.Januar 2013 und dem 31. Dezember 2014 stattfinden soll, noch nach bestehendem Recht möglich sein. Für die Fälle der regelmäßigen Meldedatenübermittlung bleibt voraussichtlich auch nach Inkrafttreten des BMeldG eine eigene Regelungsbefugnis der Länder bestehen. Derzeit finden in Berlin und Brandenburg redaktionelle Anpassungen der Meldedatenübermittlungsverordnungen an den Rundfunkbeitragsstaatsvertrag statt.

III. Berlin

Rundfunkbeitragsstaatsvertrag

Am 1. Januar 2013 wird der Rundfunkbeitragsstaatsvertrag (RBeitrStV) in Kraft treten. Die Übergangsvorschriften nach § 14 Abs. 1, 2 und 6 RBeitrStV gelten bereits seit 1. Januar 2012.

Gemäß § 9 Abs. 2 RBeitrStV wird die zuständige Landesrundfunkanstalt ermächtigt, Einzelheiten des Verfahrens

1. der Anzeigepflicht,
2. zur Leistung des Rundfunkbeitrags, zur Befreiung von der Rundfunkbeitragspflicht oder zu deren Ermäßigung,
3. der Erfüllung von Auskunfts- und Nachweispflichten,
4. der Kontrolle der Beitragspflicht,
5. der Erhebung von Zinsen, Kosten und Säumniszuschlägen und
6. in den übrigen in diesem Staatsvertrag genannten Fällen

durch Satzung zu regeln. Die Satzung bedarf der Genehmigung der für die Rechtsaufsicht zuständigen Behörde und ist in den amtlichen Verkündungsblättern

der die Landesrundfunkanstalt tragenden Länder zu veröffentlichen. Die Satzungen der Landesrundfunkanstalten sollen übereinstimmen.

Derzeit erarbeiten die Landesrundfunkanstalten den Entwurf der Beitragssatzung. Dabei findet eine enge Abstimmung mit den Rundfunkdatenschutzbeauftragten und mit den für die Datenschutzkontrolle beim Rundfunkgebühren- bzw. –beitragseinzug zuständigen Landesdatenschutzbeauftragten von Bremen, Hessen, Berlin und Brandenburg statt.

IV. Gerichtsverfahren
Unterlassungsbegehren des VZBV in Sachen KiKa-Online-Gewinnspiele

Mit Schreiben vom 14. Oktober 2011 hat der Bundesverband der Verbraucherzentralen und Verbraucherverbände (VZBV) den Mitteldeutschen Rundfunk - gestützt auf das Gesetz gegen den unlauteren Wettbewerb (UWG) - wegen der Datenabfrage für Online-Gewinnspiele des KI.Ka abgemahnt. Dabei geht es um die Praxis des Ki.Ka, bei Gewinnspielen von den Kindern neben der Antwort den Namen, das Alter und den Wohnort abzufragen. 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.

Nach Ansicht des Arbeitskreises von ARD, ZDF und DLR (AK DSB), der den Kinderkanal in datenschutzrechtlichen Fragen intensiv betreut, entspricht die dort praktizierte Datenerhebung bei Gewinnspielen den Anforderungen der sparsamen Datenerhebung. Im Übrigen ist nicht ersichtlich, dass der Ki.Ka durch die Erhebung der Daten einen Wettbewerbsvorteil erlangt. Formalrechtlich stellt sich überdies die Frage, ob das UWG hier überhaupt anwendbar ist.

Inzwischen hat der VZBV vor dem Landgericht Leipzig Klage erhoben.

C. Datenschutz und Datensicherheit im rbb

I. Interne Regelungen

1. Dienstanweisung zur Auftragsdatenverarbeitung

In meinem letzten Tätigkeitsbericht hatte ich über die Änderung des Berliner Datenschutzgesetzes informiert. Unter anderem sind in § 3 die Anforderungen an die Auftragsdatenverarbeitung verschärft worden.

Über ein Jahr lang habe ich mich zusammen mit der Abteilung Organisation und IT (OUI) und dem IT-Sicherheitsbeauftragten um eine Anpassung der **rbb**-Richtlinien für den Einsatz von Externen bei der Wartung von IT- und TK-Systemen (**rbb**-Wartungsrichtlinien) an die neue Gesetzeslage bemüht. Dabei mussten wir uns mit Bedenken insbesondere der Abteilung Einkauf auseinandersetzen. Inzwischen sind sämtliche Einwände ausgeräumt und die neue Wartungsrichtlinie ist in Kraft.

Da es neben den Wartungsarbeiten eine Vielzahl anderer Auftragsdatenverarbeitungsverhältnisse im **rbb** gibt, benötigen wir dringend eine allgemeine Dienstanweisung zur Auftragsdatenverarbeitung. Inzwischen haben die Abteilung OUI und ich von der Geschäftsleitung den Auftrag, eine entsprechende Dienstanweisung zu erarbeiten.

2. Dienstanweisung zur IT-Sicherheit

Im **rbb** fehlt bislang eine Organisationsstruktur des IT-Sicherheitsmanagements, wie sie in anderen Landesrundfunkanstalten – z.B. MDR und WDR - seit längerem existiert. Die Abteilung OUI hat dazu in enger Zusammenarbeit mit mir einen Vorschlag und den Entwurf einer Dienstanweisung zur Gewährleistung der IT-Sicherheit – „Dienstanweisung IT-Sicherheit“ - erarbeitet. Dieser wird in Kürze der Geschäftsleitung unterbreitet.

3. Dienstanweisung für die Nutzung von IT

Im **rbb** fehlt bislang auch eine Dienstanweisung für die Nutzung von PC und mobilen Endgeräten. Zwar existieren bereits einige Regelungen hierzu. Diese müssen jedoch vereinheitlicht und ergänzt werden. Auch in dieser Angelegenheit ist die Abteilung OUI derzeit in enger Abstimmung mit mir tätig.

4. Dienstvereinbarung zum Betrieblichen Eingliederungsmanagement

Mit Wirkung zum 1. September 2011 hat der **rbb** eine Dienstvereinbarung zum betrieblichen Eingliederungsmanagement (BEM) im **rbb** in Kraft gesetzt.

Nach § 84 Abs. 2 Sozialgesetzbuch (SGB) IX ist jeder Arbeitgeber verpflichtet, bei Beschäftigten, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, das Betriebliche Eingliederungsmanagement einzuleiten. Das Betriebliche Eingliederungsmanagement dient der gezielten Wiedereingliederung langzeiterkrankter Mitarbeiterinnen und Mitarbeiter in den Arbeitsprozess. Dem Personalrat ist die Aufgabe zugewiesen darüber zu wachen, dass der Arbeitgeber die ihm nach dieser Vorschrift obliegenden Verpflichtungen erfüllt. In einem bemerkenswerten Beschluss vom 7. Februar 2012 hat das Bundesarbeitsgericht festgestellt, dass die Mitteilung der Namen der für die Durchführung eines BEM in Betracht kommenden Arbeitnehmer an den Betriebsrat zur Durchführung der sich aus § 80 Abs. 1 Nr. 1 Betriebsverfassungsgesetz, § 84 Abs. 2 Satz 7 SGB IX ergebenden Überwachungsaufgaben erforderlich ist. Der Arbeitgeber muss dem Betriebsrat die Namen der Arbeitnehmer mit Arbeitsunfähigkeitszeiten von mehr als sechs Wochen im Jahreszeitraum auch dann mitteilen, wenn diese der Weitergabe nicht zugestimmt haben (BAG Der Betrieb 2012, 1517 ff.). Diese Rechtsprechung ist auf die Personalräte unmittelbar übertragbar.

Die Dienstvereinbarung beschreibt die Rahmenbedingungen und das Verfahren des BEM. Sie soll dazu beitragen, bei allen Beteiligten Vertrauen zu schaffen und ein transparentes Verfahren zu gewährleisten.

An den Vorbereitungsarbeiten zur Dienstvereinbarung war ich beteiligt. Dabei habe ich darauf geachtet, dass die Freiwilligkeit des BEM gewahrt wird. Die Betroffenen können das BEM ohne Angabe von Gründen ablehnen oder trotz erfolgter Zustimmung abbrechen, ohne dass dies arbeitsrechtliche und/oder dienstrechtliche Maßnahmen zur Folge hat. Sie können auch selbst bestimmen, welche Personen am BEM beteiligt werden (z. B. Personalrat, Frauenvertreterin, Schwerbehindertenvertreterin oder Betriebsarzt).

Zum Umgang mit den erhobenen personenbezogenen Daten gilt nach Ziffer 4 der Dienstvereinbarung:

- Alle Beteiligten am BEM sind zur Vertraulichkeit verpflichtet.
- Die Personalabteilung vermerkt in der Personalakte lediglich, ob sie ein BEM eingeleitet hat, ob die bzw. der Betroffene zugestimmt oder abgelehnt hat und wann das BEM abgeschlossen wurde. Die Personalabteilung vernichtet diesen Vermerk drei Jahre nach Abschluss des Verfahrens.
- Alle übrigen Unterlagen, wie z. B. Gesprächsvermerke, Protokolle oder sonstiger Schriftwechsel, sind nicht Gegenstand der Personalakte. Sie werden beim jeweils zuständigen Referenten der Personalabteilung aufbewahrt. Die betroffenen Mitarbeiterinnen und Mitarbeiter erhalten auf Verlangen Einblick in die Unterlagen.
- Eine Weitergabe von personenbezogenen Daten an Dritte (z. B. das Integrationsamt) ist nur mit schriftlicher Einwilligung der bzw. des Betroffenen zulässig.
- Die Anhörung von behandelnden Ärzten ist nur zulässig, wenn die bzw. der Betroffene dem ausdrücklich zustimmt und die Ärzte schriftlich von ihrer Schweigepflicht entbindet.
- Alle personenbezogenen Daten zum BEM werden drei Jahre nach Abschluss des Verfahrens qualifiziert vernichtet oder der/dem Betroffenen übergeben.
- Im Übrigen beachten alle am Verfahren Beteiligten die jeweils geltenden datenschutzrechtlichen Bestimmungen.

5. Dienstvereinbarung für das neue Dispositionssystem

Die in meinen früheren Berichten bereits erwähnten jahrelangen Verhandlungen zum neuen Dispositionssystem zwischen Geschäftsleitung und Personalrat sind mit einer gütlichen Einigung vor der Einigungsstelle beendet worden.

In diesem Zusammenhang musste die Dokumentation des vom IT-Sicherheitsbeauftragten nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erstellten IT-Sicherheitskonzepts auf Forderung der Sachverständigen des Personalrats aus für mich nur begrenzt nachvollziehbaren Gründen redaktionell überarbeitet werden. Außerdem wurde auf eine entsprechende Forderung des Personalrats hin ein von mir komplett ausformulierter rund 50seitiger Powerpoint-Vortrag zum Datenschutz als Anlange zur Dienstvereinbarung genommen. An der Sinnhaftigkeit, einen ausformulierten Vortrag zur Anlage einer Dienstvereinbarung zu machen und damit (zumindest theoretisch) den Inhalt der Datenschutzschulungen auf Dauer „einzufrieren", habe ich Zweifel.

Nach meiner Information ist das Dispositionssystem bis heute nicht in den Regelbetrieb gegangen.

6. Umsetzung der SAP-Dienstvereinbarungen

Nach wie vor ist die Umsetzung der in den aktuellen SAP-Dienstvereinbarungen vereinbarten Löschfristen für personenbezogene Daten technisch nicht sichergestellt. Ich fordere hier seit Jahren ein Konzept. Im Jahr 2009 (!) wurde mir von der Abteilung OUI mitgeteilt, dass ein Tool geprüft würde, mit dem die Daten gelöscht werden könnten. Ein abschließendes Ergebnis ist mir trotz regelmäßiger Nachfragen bis heute nicht mitgeteilt worden.

II. Aktuelle IT-Projekte

1. Elektronisches Dateienverzeichnis

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

Bislang verfüge ich nicht über die elektronische Version eines Verzeichnisses mit Beschreibungen und Verzeichnissen zu allen Datenverarbeitungsprogrammen, die beim **rbb** eingesetzt werden und mit denen personenbezogene Daten verarbeitet werden.

Die Abteilung OUI hat mir in dieser Angelegenheit Unterstützung zugesagt. Im Rahmen der Erneuerung des Windows-Fileservices wird es neue Verzeichnisstrukturen geben. Alle vorhandenen Dateien und Verzeichnisse werden auf die neuen Windows-Server übertragen. In diesem Zusammenhang soll auch mein Anliegen berücksichtigt werden. Der IT-Sicherheitsbeauftragte und der Projektleiter werden im September 2012 in dieser Sache auf mich zukommen.

2. Konzeption von technischen Betriebsräumen

Eine Prüfung der Serverräume durch die Revision hat im Herbst 2011 ergeben, dass die technischen und organisatorischen Maßnahmen zur Sicherheit der Serverräume nicht vollständig den Empfehlungen des BSI entsprechen.

Daraufhin wurde ein Projektteam mit der Erarbeitung von Vorschlägen zur Optimierung der physikalischen Sicherheit beauftragt. Ich konnte die Belange des Datenschutzes in die entsprechenden Planungen einbringen. Insbesondere haben sich das Projektteam und die Steuerungsgruppe meiner Empfehlung angeschlossen, sämtliche Serverräume, in denen personenbezogene Daten verarbeitet werden, mit einem elektronischen Zugangssystem auszustatten. Die Umsetzung soll allerdings in ei-

nem separaten Projekt unter Führung der Hauptabteilung Gebäudemanagement erfolgen. Ich hoffe, dass die beschlossenen Maßnahmen nun zeitnah umgesetzt werden.

3. Projekt der Abteilung OUI „Nutzerfreundlicher Arbeitsplatz“

Die Abteilung OUI betreibt derzeit ca. 4.000 PC-Arbeitsplätze und Notebooks mit dem Betriebssystem Windows XP und Office 2003. Das Betriebssystem Windows XP ist seit mehr als 8 Jahren im Einsatz. Der Hersteller Microsoft beendet den Support für XP und Office 2003 im April 2014.

Ab Sommer 2012 bis Ende 2013 sollen alle PC-Arbeitsplätze auf geeignete Hardware, das neue Microsoft Betriebssystem Windows 7 sowie die neue Office-Version 2010 umgestellt werden. Auch die Kommunikationsplattform Lotus Notes wird in diesem Zuge aktualisiert und auf die Version 8.5 umgestellt.

In dieser Angelegenheit bin ich mit der Abteilung OUI im Kontakt. Gemeinsam haben wir festgelegt, welche der neuen Funktionen von Lotus Notes in Zukunft bei uns genutzt werden können und wie die Nutzung erfolgen soll. Auf die Funktion „Rückholen von Mails“ werden wir gänzlich verzichten, da das System nicht unterscheiden kann, ob Mails bereits vom Adressaten geöffnet wurden oder nicht. Die Rückholung von bereits geöffneten Mails durch den Absender halte ich mit dem Deutschen Recht nicht für vereinbar.

4. Pilotprojekt „Video-HiRes-Archiv“

Im **rbb** findet derzeit das Pilotprojekt „Video-HiRes-Archiv“ statt. Ziel des Pilotprojektes ist es, filebasierte Arbeitsabläufe im Fernseharchiv und den betroffenen Redaktionen zu erproben. Im Pilotbetrieb werden die 30-minütigen Hauptausgaben der „Abendschau“ und von „Brandenburg aktuell“ und die Spätausgaben von „rbb aktuell“, die bereits heute in dem System DPS filebasiert mitgeschnitten werden, als Videofiles archiviert. Hierzu werden die DPS-Mitschnitte nach der jeweiligen Sendung an das Archivsystem im IVZ übergeben. Die Mitschnitte werden im Anschluss

von den Dokumentaren im Fernseharchiv mit sog. Metadaten erweitert, in Beiträge segmentiert und an die Fernseharchivdatenbank gemeldet. Für die Mitarbeiterinnen und Mitarbeiter in den Redaktionen wird zukünftig eine Recherche, Vorschau und Bestellung von Videofiles über den Medienbroker möglich sein. Die über den Medienbroker bestellten HiRes-Videofiles werden anschließend für DPS Potsdam oder DPS Berlin bereitgestellt.

Darüber hinaus soll im Rahmen des Pilotprojekts im Berliner Archivumspielraum die Digitalisierung von Bändern über die Software von S4M erprobt werden. Dort soll zudem die Ausspielung auf Band für Redaktionen getestet werden, die zukünftig nicht filebasiert arbeiten werden. Ein weiterer Bestandteil der Erprobung der Software ist die Auslieferung von Files an den ARD-Videofiletransfer inklusive direktem Verschicken an andere ARD-Anstalten bzw. an die **rbb**-Sendeabwicklung. Außerdem wird die Übergabe von Tonspuren an die Hörfunkproduktionssysteme sowie die Archivierung von HD-Videofiles Gegenstand des Pilotprojekts sein.

Der IT-Sicherheitsbeauftragte und ich haben dem Probebetrieb unter folgenden Voraussetzungen zugestimmt:

Für den Zugang zum SSM VPMS MediaCenter und den PreviewClient werden personalisierte Logins eingerichtet. Diese sind gleichlautend zu den FESAD Logins. Alle Archivmitarbeiterinnen und –mitarbeiter haben in S4M die gleichen Rechte, da Rechte und Rollen über die übergeordnete FESAD Benutzerverwaltung vergeben werden. Im S4M-System werden keine personenbezogenen Daten der Anwenderinnen gespeichert, sondern ausschließlich journalistische (Inhalts-)Daten. Alle personenbezogenen Daten werden wie bisher in FESAD gespeichert. Der S4M-PreviewClient, welcher auf den Clientrechnern im Archiv installiert ist, schreibt technische Logfiles auf die lokale Festplatte. Diese Logfiles enthalten auch das Userkürzel des angemeldeten Users. Diese Logfiles werden spätestens nach 30 Tagen automatisch überschrieben. Die serverseitigen Logfiles der S4M-Module werden im IVZ nach 2 Wochen auf einen nur dem IVZ zugänglichen zentralen Share gesammelt. In diesen Logfiles werden keine Benutzerdaten geloggt. Außerdem sind sie nur für IVZ-Administratoren zugänglich. Das IVZ hat alle S4M-VPMS- und Ar-

chivkomponenten durch eine Firewall geschützt. Alle VPMS-Server, die Windows-Betriebssysteme haben, wurden mit Virenscannern versehen.

5. Archimedes-Textdatenbank

In meinem letzten Tätigkeitsbericht habe ich darüber informiert, dass der **rbb** mit den Kooperationspartnern WDR, Radio Bremen, SWR, SR, NDR und DW die verschiedenen Pressearchivsysteme auf das System „Archimedes" beim WDR überführt hat. Da das IT-Sicherheitskonzept des WDR im letzten Jahr erst in Teilen vorlag, konnte ich zunächst nur einen Probebetrieb befürworten.

Im Dezember 2011 erhielt der **rbb** das vollständige Konzept. Nach gemeinsamer Prüfung mit dem IT-Sicherheitsbeauftragten konnte ich den Regelbetrieb befürworten.

6. Neue Hörfunkdatenbank

Innerhalb der ARD ist eine neue Hörfunkdatenbank (HFDB) unter der Federführung des SWR entwickelt worden, mit der das alte Großrechnersystem abgelöst wurde.

Nachdem der SWR diese Datenbank bereits im August 2009 eingeführt hat, sind HR, SR, NDR, DW, BR und DLR im Jahr 2011 als weitere Rundfunkanstalten gefolgt. Ende 2011 erfolgte schließlich auch beim **rbb** der Umstieg auf die neue Hörfunkdatenbank.

Die Hörfunkdatenbank hat eine mehrschichtige Architektur. Sie wird serverseitig vom IVZ betrieben. Grundsätzlich sind zwei Clients zu unterscheiden. Zum einen handelt es sich um den „Erfassungsclient", der die Datenerfassung, Expertenrecherche und Ausleihe ermöglicht. Dieser Client kommt nur innerhalb der Abteilung Archive und Dokumentation und an ausgewählten Plätzen in den Redaktionsarchiven zum Einsatz. Zum anderen existiert der sogenannte „Webclient", der den Redaktionen in anderen Anstalten u. a. die Recherche ermöglicht. Der Webclient wird nur übergangsweise bis zur Inbetriebnahme der sog. Industriedatenbank genutzt.

Für die allgemeine Recherche in den Redaktionen und für Bestellungen und Digitalisierungsanfragen wird weiterhin der Medienbroker genutzt, dessen Nutzung nur Journalistinnen und Journalisten gestattet ist.

Am 27. Oktober 2011 haben der IT-Sicherheitsbeauftragte und ich nach einer praktischen Vorführung und Sichtung der Unterlagen dem Probebetrieb für die neue Hörfunkdatenbank zugestimmt. Allerdings haben wir deutlich gemacht, dass für die Verlängerung des Probebetriebs bzw. für den Regelbetrieb noch folgende Punkte zu klären sind:

Es darf keine allgemeine Rolle „Gast" geben, sondern nur entsprechend eingerichtete Systemaccounts. Die Passwortkonventionen müssen den Empfehlungen des BSI entsprechen. Es muss einen erzwungenen Passwortwechsel nach 90 Tagen geben. Es muss geklärt werden, welche Logfiles beim Betrieb der Hörfunkdatenbank anfallen. Die sog. Lebensdaten der Urheber und Mitwirkenden sollten zumindest beim Medienbroker im Wortbereich ausgeblendet werden. Vom IVZ ist das Betriebskonzept zu erstellen.

7. Einführung der Archivsoftware ACTApro im Projekt Unternehmens- und Historisches Archiv

Im **rbb** gibt es die Anforderung, die aktuellen Schriftgutbestände entsprechend den Aufbewahrungsfristen und Archivalientypen befristet zu archivieren und die historischen Schriftgutbestände auf Dauer zu erhalten. Ziel des neuen Projektes ist es, die befristet im Zwischenarchiv aufzubewahrenden Schriftgutbestände in einer Datenbank zu verzeichnen, um einen Teil davon in einem weiteren Schritt nach Bewertung und Auswahl, „virtuell" in das Historische Archiv zu überführen. Dort soll das Archivgut inhaltlich erschlossen und der Nutzung zugeführt werden. Derzeit ist eine adäquate Softwarelösung dafür nicht vorhanden, der Aufbau eines Schriftgutarchivs wird erst im Verlauf des Projekts realisiert. Für die Kurzerfassung der Metadaten wie Signatur, Titel, Laufzeiten und Provenienz im Zwischenarchiv sowie eine anschließende Erschließung im Historischen Archiv (bestehend aus Metadaten der Kurzerfassung, ergänzt um Inhaltserschließung inklusive Deskriptorenvergabe und

Thesauruseintrag) wird eine Datenbank benötigt. Diese soll die zurzeit geführten Excel-Listen ersetzen. Die Projektleiterin hat sich nach einem Testeinsatz und Vergleich für die Software ACTApro ausgesprochen. Auch der Bayerische Rundfunk wird ACTApro einführen.

Es ist beabsichtigt, die Software ACTApro zunächst für eine Pilotphase bis Mitte 2013 einzusetzen.

Der IT-Sicherheitsbeauftragte und ich haben der Projektleiterin in einem ersten Gespräch erläutert, welche Informationen wir im Einzelnen für die Erarbeitung eines IT-Sicherheitskonzepts und die datenschutzrechtliche Bewertung benötigen. Hier stehen noch wesentliche Dinge aus.

8. Einführung eines Videokonferenzsystems

Um Fahrten zwischen den einzelnen Standorten zu minimieren, hat der **rbb** Anfang des Jahres 2012 ein neues Videokonferenzsystem in Betrieb genommen.

Vor Inbetriebnahme muss das System jeweils von einem Konferenzleiter gestartet bzw. beendet werden. Außerhalb der Konferenzzeiten werden weder Bild- noch Tonsignale übertragen. Das System ist nur in bestimmten Konferenzräumen an den Standorten Berlin, Potsdam, Frankfurt/Oder und Cottbus zugänglich. Perleberg und Prenzlau erhalten den Zugang zum Videokonferenzsystem über einen Konferenz-PC, der an das System angebunden ist. Dieser PC wird ausschließlich hierfür genutzt und eingerichtet. Vor und während der Konferenzschaltung wird dies deutlich durch ein Schild sichtbar gemacht, da die Räumlichkeiten einen eigens für Konferenzen zu nutzenden Raum nicht hergeben.

Das Bild- und/oder Tonsignal kann nicht mitgeschnitten werden. Verbindungsdaten werden standardmäßig auf dem Vermittlungsserver gespeichert. Die Verbindungsdaten umfassen ausschließlich die Anschlussnummern des jeweiligen Konferenzsystems (interne **rbb**-Telefonnummern dieses Systems). Daraus lassen sich keine Erkenntnisse über die teilnehmenden Personen ziehen. Das Steuergerät der Video-

konferenzanlage befindet sich im Serverraum in Potsdam. Das Gerät wird nur von zwei Administratoren bedient. Der Zugang zu dem Gerät ist durch Passwort geschützt. Die Aktivitäten der Administratoren werden mitprotokolliert. Die Verbindungsdaten werden ausschließlich für Datensicherheitszwecke maximal 7 Tage aufbewahrt.

Am 20. Januar 2012 hat die Abteilung OUI dem stellvertretenden Datenschutzbeauftragten und mir im Beisein des IT-Sicherheitsbeauftragten das Videokonferenzsystem präsentiert. Dabei konnten wir uns davon überzeugen, dass die Datenübertragung während der Videokonferenz über das Hausnetz über einen logisch getrennten Kanal im Datennetz erfolgt. Dadurch ist technisch ausgeschlossen, dass sich normale PC mit Webcam dazuschalten können. Es ist derzeit auch technisch ausgeschlossen, dass sich Personen von außen per Telefon dazuschalten können.

Ich habe dem Einsatz des Videokonferenzsystems unter folgenden Bedingungen zugestimmt:

Schon bei der Einladung der Teilnehmerinnen und Teilnehmer zu einer Konferenz sollte deutlich gemacht werden, dass es sich um eine Videokonferenz handelt. Zusätzlich zu dem Schild an den Räumlichkeiten, die auf eine Videokonferenz hinweisen, ist durch geeignete Maßnahmen (Kameraeinstellung, Rollos an Türen und Fenstern u.ä.) sicherzustellen, dass Passanten nicht unbemerkt bzw. ungewollt in den Kamerabereich des Videokonferenzsystems gelangen.

III. Organisatorisches

1. Datenschutz bei Kopiergeräten

Aufgrund des Hinweises eines Kollegen, wonach angeblich an unseren Kopiergeräten der Datenschutz nicht gewährleistet sei, bin ich der Frage nachgegangen, ob die seinerzeit in dem in Zusammenarbeit mit mir erstellten Leistungsverzeichnis geforderten Datensicherheitsfunktionen auch tatsächlich von unserem Vertragspartner geliefert wurden und in Funktion sind.

Am 2. April 2012 habe ich zusammen mit zwei Kollegen aus der Abteilung Infrastruktur und dem IT-Sicherheitsbeauftragten dazu ein Gespräch mit dem regionalen Servicemanager des Herstellers der Geräte Toshiba geführt. Als Ergebnisse des Gesprächs konnten wir folgendes festhalten:

Die im **rbb** vorhandenen einfachen Kopiergeräte sind mit einer Festplatte ausgestattet. Die Daten werden dort stark verschlüsselt zwischengespeichert. Nach dem Kopieren werden sie mit einem sog. Data-Overwrite-Kit überschrieben. Damit wird das nachträgliche Auslesen verhindert. Bei der nächsten Wartung Ende 2012 wird der Status zur Verschlüsselung und dem Data-Overwrite bei den im **rbb** vorhandenen Kopierergeräten durch Toshiba ermittelt und dem **rbb** zur Prüfung vorgelegt.

Neben den Kopiergeräten ist im **rbb** allerdings inzwischen auch eine Reihe von sog. Multifunktionsgeräten in Gebrauch. Diese Geräte sind zumindest zum Teil auch an unser Netzwerk angeschlossen. Zusammen mit dem IT-Sicherheitsbeauftragten bin ich der Auffassung, dass für die Nutzung dieser Geräte jetzt dringend ein Gesamtkonzept einschließlich der Datenschutz- und Datensicherheitsmaßnahmen erarbeitet werden muss. Ich habe dies der zuständigen Abteilung OUI angezeigt.

2. Buchung von Bahnfahrten über das Firmenkundenportal der DB bahn.corporate

Seit Mitte 2011 besteht im **rbb** die Möglichkeit, alternativ zum bestehenden Buchungsverfahren mit Formular oder per Telefon über den Reisedienstleister BCD Travel Bahnkarten für dienstliche Zwecke online über das Firmenkundenportal der DB bahn.corporate zu buchen.

Das Verfahren ist mit dem IT-Sicherheitsbeauftragten und mir abgestimmt worden. Es ist sichergestellt, dass im Zusammenhang mit der Nutzung des Online-Portals nur diejenigen personenbezogenen Daten erhoben werden, die für den Buchungsvorgang tatsächlich benötigt werden. Die Datenübertragung erfolgt über das Internet. Dabei wird die Datensicherheit durch eine angemessen starke Verschlüsselung

gewährleistet. In einem Merkblatt, das jedem Nutzer/jeder Nutzerin zu Beginn ausgehändigt wird, sind die organisatorischen Maßnahmen zum Datenschutz aufgelistet, die jede/r einhalten muss: Wahl eines sicheren Passwortes, regelmäßige Änderung des Passwortes, keine Weitergabe des Passwortes an Dritte sowie Abmeldung vom System bzw. Sperrung bei Abwesenheit.

3. Akkreditieren – Fotos aus Hausausweisdatei

Jede Mitarbeiterin/jeder Mitarbeiter erhält zu Beginn ihrer/seiner Tätigkeit beim **rbb** einen Hausausweis, mit dem sie/er sich regelmäßig beim Empfang ausweisen muss. Die Fotos für die Hausausweise werden in der Abteilung Infrastruktur hergestellt und in digitaler Form in einer Hausausweisdatei vorgehalten, damit im Falle des Ausweisverlusts problemlos Ersatz geschaffen werden kann. Die Fotos dürfen entsprechend ihrem bei der Herstellung vereinbarten Zweck ausschließlich für die Dienstausweise verwendet werden.

In der Praxis hat sich die Notwendigkeit ergeben, im Zusammenhang mit Veranstaltungen Mitarbeiterinnen und Mitarbeiter aus der Produktion kurzfristig zu akkreditieren. In bestimmten Fällen ist dafür auch ein Bild erforderlich.

Zusammen mit den Kollegen aus der Abteilung Bild habe ich eine Einverständniserklärung entwickelt, die es ermöglicht, das Foto, welches für den Hausausweis angefertigt wurde, auch zu Zwecken der Akkreditierung zu verwenden.

4. Fahrten zwischen Wohnort und Arbeitsstätte mit rbb-Fahrzeugen

Nutzen **rbb**-Mitarbeiter **rbb-**Fahrzeuge für die Wahrnehmung auswärtiger Termine, so kommt es häufig vor, dass die Dienstfahrzeuge über Nacht mit nach Hause genommen und erst am nächsten Tage beim **rbb** wieder abgegeben werden.

Fahrten mit **rbb**-Fahrzeugen zwischen Wohnort und Arbeitsstätte stellen jedoch geldwerte Vorteile dar und müssen versteuert werden. Im Rahmen einer Lohnsteueraußenprüfung, die im Dezember 2010 stattfand und bei der der Sachverhalt

„Fahrtkostenersatz für Fahrten zwischen Wohnung und Arbeitsstätte“ geprüft worden war, wurde beanstandet, dass es dazu im **rbb** noch keine Regelung gab. Bis zu der Prüfung ging der Fahrdienst bei Fahrzeugbuchungen immer vom ausschließlich dienstlichen Zweck der Fahrt aus. Um der Lohnsteueraußenprüfung Genüge zu tun und sich nicht möglicherweise dem Vorwurf der Steuerhinterziehung auszusetzen, hat der Bereich Flächen- und Fuhrparkmanagement in Abstimmung mit mir ein Verfahren entwickelt, bei dem den Mitarbeiterinnen und Mitarbeitern in begründeten und vom Vorgesetzen bestätigten Ausnahmefällen auf Antrag Fahrten zwischen Arbeitsstätte und Wohnort gestattet werden. Per Dokumentenausdruck werden die im Quartal insgesamt gefahrenen Kilometer zwischen Wohnort und Arbeitsstätte an die Personalabteilung für die Abrechnung übergeben. Es werden keine Schnittstellen zwischen dem Fahrzeugdispositionssystem und dem in der Personalabteilung verwendeten IT-Systemen geschaffen. Auswertungen zur Leistungs- und Verhaltenskontrolle sind nicht erlaubt.

IV. Datenschutz und Datensicherheit in der Personalwirtschaft

1. Evaluation der Mitarbeitergespräche

Seit März 2005 gibt es im **rbb** formalisierte Mitarbeitergespräche. Grundlage ist die „Dienstvereinbarung Mitarbeitergespräche“ vom 1. März 2005. Im Sommer 2011 haben sich die Personalabteilung und der Personalrat darauf verständigt, eine anonyme Befragung mit Hilfe einer Funktion in unserem E-Mail System Lotus Notes durchzuführen. Sowohl der Inhalt des Fragebogens als auch das konkrete Procedere wurden mit mir abgestimmt. Bei dem Abruf der elektronischen Auswertungen durch den Administrator waren neben zwei Vertretern der Personalabteilung auch eine Vertreterin des Personalrats und ich anwesend. Wir konnten uns von der Anonymität der Auswertung vor Ort überzeugen.

2. Kommunikation im rbb – Projekt im Rahmen der Nachwuchsförderung

Im Rahmen der Nachwuchsförderung wurde Anfang 2012 ein Projekt zum Thema „Kommunikation im **rbb**: Wie wird sie wahrgenommen? Wie lässt sie sich verbes-

sern?“ gestartet. In diesem Zusammenhang hat die Abteilung Presse und Information eine Beraterin für konstruktive Kommunikation mit der Durchführung und wissenschaftlichen Auswertung von Interviews mit ausgewählten repräsentativen Mitarbeitern der verschiedenen Direktionen und Hierarchieebenen, Frauen und Männern, sowohl ehemalige ORB- als auch SFB-Mitarbeiterinnen und –Mitarbeitern, festen und freien Mitarbeiterinnen und Mitarbeitern beauftragt. Das organisatorische Procedere hat die aus Nachwuchskräften bestehende Projektgruppe mit mir abgestimmt. Die Interviews, an denen niemand aus der Projektgruppe teilgenommen hatte, wurden aufgezeichnet und transkribiert. Die anschließende wissenschaftliche Auswertung erfolgte anonymisiert. Nach der Transkription wurde die Tonaufnahme nicht weiterverwendet, sondern von der externen Beraterin verschlossen aufbewahrt. Nach Abschluss des Projekts im September 2012, spätestens zum 31. Dezember 2012, werden die Tonaufnahmen gelöscht.

3. Hospitanzen

Seit Beginn des Jahres 2012 können die Mitarbeiterinnen und Mitarbeiter durch eintägige Hospitanzen in den Bereichen des Hauses, die sie noch nicht kennen, neue Eindrücke und Erfahrungen sammeln.

Zur Auswertung des Hospitanzprogramms haben die Projektleiter in Abstimmung mit den Mitarbeitervertretungen und mit mir einen Evaluationsbogen entworfen. Das Feedback ist freiwillig. Die Auswertung erfolgt anonym.

4. Datenübermittlung von Mitarbeiterinnen und Mitarbeitern an Sozialleistungsträger

Im Jahr 2011 hat sich eine Kollegin bei mir über die Personalabteilung beschwert. Diese hatte auf Anforderung der Stadt Hannover zur Ermittlung von Unterhaltspflichten sämtliche Honorardaten der freien Mitarbeiterin für die zurückliegenden zwei Jahre übermittelt, ohne die Mitarbeiterin selbst zu informieren.

Nach Prüfung des Vorgangs habe ich ihr mitgeteilt, dass der Arbeitgeber gemäß § 117 Abs. 3, Abs. 4 SGB XII zur Auskunft gegenüber den Sozialleistungsträgern verpflichtet ist. Dabei beschränkt sich seine Pflicht zur Auskunft allerdings auf diejenigen Daten, die zur Ermittlung der Unterhaltspflicht erforderlich sind. Verweigert er diese Auskunft, so handelt er ordnungswidrig, wenn kein Rechtfertigungsgrund vorliegt.

Aus Tz. 4.3. Satz 4 unserer Datenschutz-Dienstanweisung ergibt sich eine Benachrichtigungspflicht. Danach ist die/der Betroffene über den Inhalt und Empfänger der erteilten Auskunft zu unterrichten, es sei denn, es handelt sich um eine Sammelanfrage, und die Unterrichtung ist mit einem unverhältnismäßigen Aufwand verbunden. Auf diese Vorschrift habe ich die Personalabteilung hingewiesen. Sie hat zugesichert, zukünftig in vergleichbaren Fällen ihrer Benachrichtigungspflicht nachzukommen.

V. Datenschutz bei den Programmangeboten

1. Datenschutz bei Social-Media-Angeboten

Auf seiner Sitzung am 26. April 2012 hat der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) den Leitfaden zu Datenschutz und Datensicherheit bei Social-Media-Angeboten der Rundfunkanstalten verabschiedet, den eine ad hoc-Arbeitsgruppe aus Datenschützern und Onlinern von ARD und ZDF unter meiner Leitung erarbeitet hat (Anlage). Der Leitfaden löst unser entsprechendes Papier aus 2009 ab. Neu sind insbesondere die Ausführungen zur Nutzung von Social Media Plattformen Dritter und zum Angebot von Apps.

Ich habe den Leitfaden allen betroffenen Stellen im **rbb** zur Kenntnis gegeben.

2. Fotos und Filme auf Facebook und im Internet

Auf der Personalversammlung am 31. Mai 2011 wurde über das Thema Fotos und Filme im Internet und auf Facebook gesprochen. Dabei war u. a. die Frage aufge-

worfen worden, ob Reporter von **rbb**-Mitarbeiterinnen und –Mitarbeitern Fotos und Filme herstellen dürfen, die anschließend in Facebook oder an anderer Stelle im Internet veröffentlicht werden.

Dazu habe ich wie folgt Stellung genommen:

Fotos und Videos dürfen auch im Internet grundsätzlich nur mit Einwilligung der Dargestellten verbreitet werden. 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. Von allen anderen Kolleginnen und Kollegen wird eine ausdrückliche Einwilligung benötigt. Zwar genügt grundsätzlich eine mündliche Einwilligung. Im Idealfall liegt aber eine entsprechende schriftliche Erklärung vor, denn im Konfliktfall trifft den Fotografen bzw. den **rbb** als Verbreiter die Beweislast dafür, dass die Einwilligung in die Veröffentlichung vorliegt.

3. Testbetrieb Reporterhandy

Anfang 2012 startete der Testbetrieb zum sog. Reporterhandy.

Da der **rbb** für die Bestückung seines Online-Angebotes eine große Anzahl von aktuellen Fotos und Videos benötigt, hat die Geschäftsleitung entschieden, Fernseh- und vor allem auch Hörfunkreporter mit redaktionsgebundenen Smartphones als Reporterhandys auszurüsten. Die Reporter nehmen damit Fotos und Videos auf, die sie den Online-Redakteuren per E-Mail zur Verfügung stellen. Bei Veröffentlichung des Materials erfolgt eine Honorierung.

Im Vorfeld habe ich die datenschutzrechtlichen Anforderungen definiert. Die Ausleihe und Nutzung der Geräte erfolgt auf der Basis der Dienstvereinbarung über die Nutzung mobiler Telekommunikationsgeräte. Für das Bildmaterial auf dem Handy

und für das nichtverwendete Bildmaterial im E-Mail-System wurden kurze Löschfristen vereinbart. Auswertungen des Projekts erfolgen durch den Projektleiter ausschließlich anhand anonymisierter Daten. Der IT-Sicherheitsbeauftragte hat zusätzlich die Anforderungen an die sichere Übertragung und Aufbewahrung des Bildmaterials definiert.

VI. Informationsmaßnahmen

Am 29. August 2011 fand das jährliche Datenschutzseminar für die neuen Auszubildenden beim **rbb** statt.

Am 3. und 17. Mai 2011 habe ich zusammen mit meiner Kollegin Frau Engel aus der Abteilung OUI eine datenschutzrechtliche Unterweisung für die SAP-Nutzerinnen und –Nutzer durchgeführt.

Am 7. und 8. Dezember 2011 und am 3. Februar 2012 habe ich – zusammen mit dem Projektleiter Herrn Donker - jeweils eine juristische Einweisung der Nutzerinnen und Nutzer der Reporterhandys (s. dazu 5.3) – insbesondere zum Persönlichkeitsschutz - durchgeführt.

Am 14. Dezember 2011 habe ich die Nachwuchsführungskräfte zusammen mit dem IT-Sicherheitsbeauftragten in Datenschutz und Datensicherheit geschult.

D. Datenschutz bei der Rundfunkteilnehmerdatenverarbeitung

I. Allgemeines

Seit dem 1. Januar 1976 zieht die GEZ die Rundfunkgebühren für die Landesrundfunkanstalten ein. Der bei der GEZ geführte Rundfunkteilnehmer-Datenbestand umfasste per Ende Dezember 2011 rund 39,41 Millionen Teilnehmerkonten. Im Auftrag des **rbb** verwaltete die GEZ Ende 2011 insgesamt 2.845.301 Teilnehmerkonten.

Die Überwachung des Datenschutzes bei der Verarbeitung der Rundfunkteilnehmerdaten obliegt der bzw. dem für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten. Für Radio Bremen, den Hessischen Rundfunk und den **rbb** obliegt die Kontrolle der Einhaltung von Datenschutzbestimmungen der/dem jeweiligen Landesdatenschutzbeauftragten (**rbb**: Landesbeauftragter 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 BlnDSG bin ich für die ordnungsgemäße Datenverarbeitung beim **rbb** unmittelbar zuständig. Unbeschadet der Zuständigkeit des nach Landesrecht für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ist bei der GEZ gemäß § 8 Abs. 2 Satz 2 Rundfunkgebührenstaatsvertrag (RGebStV) eine betriebliche Datenschutzbeauftragte bestellt. Die betriebliche Datenschutzbeauftragte der GEZ arbeitet zur Gewährleistung des Datenschutzes mit dem/der nach Landesrecht für die jeweilige Rundfunkanstalt zuständigen Datenschutzbeauftragten zusammen und unterrichtet diese/n über Verstöße gegen Datenschutzvorschriften sowie über die dagegen getroffenen Maßnahmen.

Bei der Rundfunkteilnehmerdatenverwaltung sind meine ständigen Ansprechpartner zum einen die Abteilung Rundfunkgebühren und zum anderen die GEZ in Köln. Während mit der Abteilung Rundfunkgebühren in der Regel Einzelfälle zur Diskussion stehen, konzentriert sich die Zusammenarbeit mit der GEZ auf die Sicherstellung der Datenschutzkonformität des von dieser abzuwickelnden Massenverfahrens.

II. Auskunftsersuchen und Eingaben

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

Im Jahr 2011 hat die Datenschutzbeauftragte der GEZ folgende Vorgänge aus dem Sendegebiet des **rbb** für mich bearbeitet:

Ersuchen von Rundfunkteilnehmern um Auskunft über zu ihrer Person gespeicherte Daten:	24
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:	15
Anfragen von Finanzämtern nach Daten (insbesondere Bankverbindungen) von Rundfunkteilnehmern:	6
Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten von Rundfunkteilnehmern:	5
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz:	14
Anzahl der Vorgänge insgesamt:	**68**

Ich selbst habe in 2011 folgende Vorgänge bearbeitet:

Ersuchen von Rundfunkteilnehmern um Auskunft über zu ihrer Person gespeicherte Daten:	2
Fragen bezüglich der Herkunft von Daten (bzw. Adressen) bzw. der Berechtigung zur Datenerhebung:	4
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz:	2
Anzahl der Vorgänge insgesamt:	**7**

Hervorzuheben ist eine Eingabe Ende 2011 wegen Übermittlung von Bankdaten, die uns über den Berliner Beauftragten für Datenschutz und Informationsfreiheit erreicht hat.

Die Petentin hatte sich darüber beschwert, dass ihr von der GEZ ihre eigenen Bankdaten per Post mit der Bitte mitgeteilt worden seien, sie möge sie unterschrieben zurücksenden. Die Petentin hatte erklärt, die Abbuchung der Gebühren von ihrem Konto verlaufe seit Jahren problemlos. Sie sehe eine unnötige und erhebliche Gefahrenquelle in dieser Form der Datenübermittlung.

Dazu konnte ich Folgendes erläutern:

Anlass des Schreibens der GEZ war das sog. SEPA-Lastschriftverfahren. Den Rahmen für die Einführung der SEPA-Lastschrift bildet die EU-Richtlinie für Zahlungsdienstleistungen, die zum 1. November 2009 in Deutsches Recht umgesetzt worden ist. Bargeldlose Zahlungen innerhalb der teilnehmenden Länder sollen so weiter standardisiert werden. Mit der Einführung der SEPA-Lastschrift ist u. a. die Vorlage der handschriftlichen oder elektronisch unterzeichneten Einzugsermächtigungen gegenüber Banken, Sparkassen etc. verbunden.
Das zu erwartende, europaweit einheitliche Lastschriftverfahren schließt somit künftige Einzugsermächtigungen ohne Vorlage der handschriftlichen oder elektronischen Signatur aus. Bislang unterliegt die Erteilung einer Einzugsermächtigung keinen gesetzlichen Formerfordernissen. In vielen Fällen sind die Einzugsermächtigungen der GEZ schriftlich, per Telefax, mittels Internet oder fernmündlich erteilt worden.

Bis zum 14. Februar 2014 werden die nationalen Verfahren durch SEPA ersetzt.

Vor diesem Hintergrund hat die GEZ Ende letzten Jahres alle am Lastschriftverfahren teilnehmenden Rundfunkteilnehmer/innen per Post angeschrieben, zu deren Rundfunkteilnehmerkonto keine unterschriebene Einzugsermächtigung besteht. Dabei mussten die Angeschriebenen die zu ihrer Person bei der GEZ vorhandenen Bankdaten lediglich überprüfen und das unterschriebene Formular an die GEZ zurücksenden. Von einer Selbstausfüllung der Formulare durch die Teilnehmer hat die

GEZ – für mich nachvollziehbar - deshalb abgesehen, weil in diesem Fall die Rücklaufquote vermutlich wesentlich geringer gewesen wäre.

Die Aktion hatte den positiven Nebeneffekt, dass in vielen Fällen die Daten von Teilnehmerkonten aktualisiert werden konnten.

III. Überprüfung der Vertragsbeziehungen zwischen der GEZ und Adresshändlern durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit

Wie in meinen früheren Tätigkeitsberichten erläutert, mietet die GEZ auf der Grundlage von § 8 Abs. 4 Rundfunkgebührenstaatsvertrag regelmäßig Adressen bei privaten Adresshändlern an, um Personen, die noch nicht als Rundfunkteilnehmer gemeldet sind, per Informationsschreiben über die Rundfunkgebührenpflicht zu informieren. Dabei kommt es in Ausnahmefällen aufgrund der Zulieferung von mangelhaften Daten zu fehlerhaften Anschreiben. So ist es beispielsweise vorgekommen, dass Verstorbene angeschrieben wurden. Auch Haustiere bekamen schon Post von der GEZ.

Anlässlich einer bei ihm eingegangenen Petition im Zusammenhang mit einer Mailingmaßnahme hat sich der Beauftragte für Datenschutz und Informationsfreiheit im vergangenen Jahr allgemein dem Thema „Vertragsbeziehungen zwischen der GEZ und kommerziellen Adresshändlern“ angenommen. Es wurde gefordert, vertraglich bestimmte Intervalle für Kontrollen bei den Adresslieferanten festzulegen sowie Vertragsstrafen und ein Recht auf außerordentliche Kündigung bei Nichteinhaltung der vereinbarten Maßnahmen zur Aktualisierung von Anschriften zu vereinbaren. Ich habe gegenüber der Behörde dargelegt, dass schon heute mit Hilfe entsprechender vertragliche Vereinbarungen und regelmäßige Kontrollen der Adresszulieferer durch die Datenschutzbeauftragte und andere Mitarbeiterinnen und Mitarbeiter der GEZ Schlechtleistungen weitgehend ausgeschlossen werden können. Eine hundertprozentige Sicherheit gibt es allerdings nicht. Auf eine Nachfrage, ob Erkenntnisse zu eventuell geplanten Prüfungen der Adresslieferanten durch die

zuständigen staatlichen datenschutzrechtlichen Aufsichtsbehörden vorliegen, habe ich bislang keine Antwort erhalten.

IV. Protokollierung von Zugriffen auf Teilnehmerkonten

Im Jahr 2011 kam es aufgrund einer Indiskretion zu einer Veröffentlichung des in der Rundfunkteilnehmer-Datenbank bei der GEZ gespeicherten Anmeldeformulars eines ehemaligen Bewerbers um den Intendantenposten beim Mitteldeutschen Rundfunk. Der Informant der Zeitung, die das Anmeldeformular veröffentlicht hatte, konnte nicht ermittelt werden. In diesem Zusammenhang wurde auch die Protokollierung von Zugriffen auf Teilnehmerkonten problematisiert.

Bis dahin wurde lediglich die Bearbeitung von Vorgängen (auch Telefonvorgängen) stets im System protokolliert Hinsichtlich der Protokollierung rein lesender Zugriffe existierten bis letztes Jahr hingegen unterschiedliche Verfahren:

Bei der (nur eingeschränkten) Auskunft für die Rundfunkgebührenbeauftragten (BDONAB) wurden alle Aufrufe von Teilnehmerkonten protokolliert. Da ein Zugriff der Mitarbeiter/innen der Landesrundfunkanstalten (LRA) auf LRA-fremde Teilnehmerkonten nur im Einzelfall und nur im Rahmen der Aufgabenerfüllung des Gebühreneinzugs zulässig ist, wurden zudem alle Zugriffe auf LRA-fremde Teilnehmerkonten protokolliert. Im Falle lesender Zugriffe oder von Recherchezugriffen auf LRA-eigene Teilnehmerkonten fand hingegen keine Protokollierung statt. Gleiches galt in Bezug auf lesende Zugriffe durch GEZ-Mitarbeiterinnen.

Die GEZ ist anlässlich dieses Vorfalls dazu übergegangen, sämtliche lesenden Zugriffe der Mitarbeiter der GEZ zu protokollieren. Der AK DSB hat sich nach ausführlicher Diskussion insbesondere zur Frage der Verhältnismäßigkeit für die Protokollierung des lesenden Zugriffs auch in den Landesrundfunkanstalten als technische Maßnahme zum Datenschutz ausgesprochen.

E. Datenschutz im Informationsverarbeitungszentrum (IVZ)

Beim **rbb** wird als Gemeinschaftseinrichtung von MDR, NDR, RB, Deutschlandradio, **rbb,** SR und neuerdings auch WDR das rechtlich unselbstständige Informationsverarbeitungszentrum IVZ betrieben. Dort werden für die beteiligten Anstalten zentral Aufgaben der elektronischen Datenverarbeitung abgewickelt.

Für die Kontrolle des Datenschutzes und der Datensicherheit sind die Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Seit 1. April 2011 hat das IVZ eine hauptamtliche IT-Sicherheitsbeauftragte, Frau Fackeldey. Ihre Aufgaben umfassen neben der Umsetzung der IT-Sicherheitsvorgaben des BSI vor allem eine Begleitung aller Änderungsprozesse (z. B. Einführung neuer Systeme oder Änderung bestehender Systeme) sowie die ständige Beratung aller Mitarbeiterinnen zu den Themen der Sicherheit und regelmäßige Sensibilisierung.

Am 24. November 2011 fand beim IVZ das jährliche Treffen der Datenschutzbeauftragten der beteiligten Anstalten und des IVZ statt. Es wurde über das BSI-Re-Zertifizierungsverfahren und einige weitere datenschutzrechtlich relevante Projekte des IVZ berichtet. Außerdem wurde ein standardisiertes Verfahren für die Herausgabe von Daten an Dritte beschlossen. Der Geschäftsführer hat den Rundfunkdatenschutzbeauftragten versichert, dass für das IVZ - wie auch für die Rundfunkanstalten – die Nutung von public Clouds nicht in Frage komme. Allerdings sei die grundsätzliche Cloud-Technologie eine bereits beim IVZ eingesetzte Form, Dienstleistungen anzubringen.

F. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Der AK DSB hat im Berichtszeitraum zweimal getagt.

Auf der Sitzung bei Radio Bremen am 5. /6. Mai 2011 habe ich über die Novellierung des Berliner Datenschutzgesetzes Anfang 2011 und über die Verschärfungen der Bestimmungen zur Auftragsdatenverarbeitung berichtet. Angesichts der Tatsache, dass die GEZ stets die strengsten Datenschutzbestimmungen einhalten muss, die auch nur bei einer Landesrundfunkanstalt gelten, hat der AK DSB beschlossen, dass sämtliche Verträge zur Auftragsdatenverarbeitung bei der Gemeinschaftseinrichtung GEZ zukünftig den in § 11 Bundesdatenschutzgesetz definierten Anforderungen entsprechen müssen. Außerdem haben wir uns auf der Sitzung u. a. mit der Revision der EU-Gesetzgebung zum Datenschutz, der Reform der Rundfunkfinanzierung, mit Web-Analyse-Tools und mit Fragen zum Datenschutz bei Social Media - beschäftigt.

Auf unserer Sondersitzung am 12. September 2011 bei der GEZ in Köln haben wir uns mit verschiedenen Einzelfragen im Zusammenhang mit der Umsetzung des Rundfunkbeitragsstaatsvertrages – insbesondere mit dem in § 14 Abs. 9 RBeitrStV vorgesehenen einmaligen Meldedatenabgleich beschäftigt.

Am 10./11. November 2011 fand eine weitere Sitzung des AK DSB bei der Deutschen Welle in Bonn statt. Themen waren u.a. die EU-Gesetzgebung zum Datenschutz, das Konzept der GEZ für die Bearbeitung der Daten beim einmaligen Meldedatenabgleich Anfang 2013, Fanpages bei Facebook und die Anforderungen an den Datenschutz bei hybriden Endgeräten (HbbTV) sowie Cloud Computing.

Am 4. Oktober 2011 fand eine Telefonschaltkonferenz statt, zu der der Vorsitzende der AG Rundfunkgebührenrecht, Herr Dr. Eicher, eingeladen hatte. Gegenstand der Erörterung waren Bedenken der Landesdatenschutzbeauftragten im Hinblick auf die Datenschutzkonformität diverser Regelungen des bis dato noch nicht ab-

schließend ratifizierten Rundfunkbeitragsstaatsvertrages. An der nachfolgenden Sitzung mit einigen Landesdatenschutzbeauftragten am 6. Oktober 2011 in Mainz habe ich zusammen mit weiteren Vertreter/innen der Rundfunkdatenschutzbeauftragten teilgenommen.

Am 14. Dezember 2011 fand eine Telefonschaltkonferenz zur Novellierung der EU-Datenschutzrichtlinie statt.

Auf unserer Telefonschaltkonferenz am 30. Januar 2012 haben wir uns im Schwerpunkt mit datenschutzrechtlichen Fragen im Zusammenhang mit der neuen Satzung über das Verfahren zur Leistung der Rundfunkbeiträge beschäftigt.

II. Arbeitskreis Medien der Datenschutzbeauftragten von Bund und Ländern

Im Arbeitskreis Medien diskutieren die Datenschutzbeauftragten von Bund und Ländern unter dem Vorsitz der Brandenburgischen Datenschutzbeauftragte, Frau Dagmar Hartge, 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.

Ich habe den AK DSB auf der Sitzung des AK Medien am 6. März 2012 vertreten. Themen waren unter anderem der 15. Rundfunkänderungsstaatsvertrag, die Inkassotätigkeit der Fa. Creditreform für die Rundfunkanstalten, die Verarbeitung personenbezogener Daten bei der Nutzung der „Tagesschau-App“ und polizeiliche Recherchen in sozialen Netzwerken.

III. Teilnahme an Veranstaltungen

Am 2. Dezember 2011 habe ich am Fachgespräch „Datenschutz modernisieren“ der Bundestagsfraktion Bündnis 90/Die Grünen teilgenommen.

Berlin, 30. August 2012

gez. Anke Naujock

Anlage