



MITTELDEUTSCHER RUNDFUNK
Anstalt des öffentlichen Rechts

DATENSCHUTZBEAUFTRAGTER

**Tätigkeitsbericht des
Beauftragten für den
Datenschutz des MDR
für den Zeitraum
01.07.2013 bis 30.06.2014**

Stephan Schwarze

Inhaltsverzeichnis

1. Einleitung	4
2. Aufgaben des Datenschutzbeauftragten	6
3. Entwicklung des Datenschutzrechts	8
3.1 Europarechtliche Entwicklungen	8
3.2 Entwicklung des Bundes- und des Landesrechtes	9
4. Datenschutz im MDR	10
4.1 Vorabkontrolle Employee Self Service	10
4.2 Vorabkontrolle des Planungssystems EVIS für die HA Klangkörper	11
4.3 Datenschutz bei Angeboten des MDR auf Drittplattformen	12
4.4 Aufbewahrung von Zuschauerpost	14
4.5 HbbTV und Datenschutz	15
4.6 Rentenalter von freien Mitarbeitern	16
4.7 Sichtbarkeit von Druckaufträgen	18
4.8 Programmvergabebericht	19
5. Datenschutz beim KiKA	20
5.1 Unterarbeitsgruppe Datenschutz bei Kindern und Jugendlichen	20
5.2 Klage wegen KiKA-Gewinnspiel	22
6. Datenschutz beim Beitragsservice	23
6.1 Datenschutz im Zusammenhang mit dem Rundfunkbeitrag	23
6.2 Schulung der Regionalberater	24
7. Externe Prüfungen	25
7.1 Informationsverarbeitungszentrum (IVZ)	25
7.2 IVZ-Verwaltungsvereinbarung	25
8. Zusammenarbeit im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR	26
9. Schlussbemerkungen	27
10. Anhang	29
10.1 §§ 39 bis 42 MDR-Staatsvertrag	29
10.2 Artikel 28 und 29 EG-Richtlinie 95/46 vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr	31
10.3 §§ 11 und 14 Rundfunkbeitragsstaatsvertrag	34

10.4 §§ 7 bis 9 MDR-Rundfunkbeitragssatzung	37
10.5 Verfahrenskodex der Rundfunkbeauftragten für den Datenschutz	39
10.6 Mitglieder des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB)	42

1. Einleitung

Der Verwaltungsrat hat mich in seiner Sitzung am 18. Juni 2012 auf Vorschlag der Intendantin gemäß § 42 MDR-Staatsvertrag als Beauftragten für den Datenschutz des MDR für die Dauer von vier Jahren bestellt. Bereits im Jahr 2013 habe ich meinen ersten Tätigkeitsbericht vorgelegt. Mit diesem Bericht habe ich die Pflicht aus § 42 Abs. 8 des MDR-Staatsvertrages erfüllt, wonach der Beauftragte für den Datenschutz den Organen der Rundfunkanstalt einen Bericht über seine Tätigkeit erstatten muss. Dieser vorliegende Bericht ist der zweite meiner Amtszeit und erfolgt in Abstimmung mit dem Verwaltungsrat bereits ein Jahr nach dem ersten Bericht. In Zukunft wird der in § 42 Abs. 8 MDR-Staatsvertrag vorgesehene zweijährige Rhythmus für den Tätigkeitsbericht wieder aufgenommen.

Förmliche Beanstandungen mussten im Berichtszeitraum nicht ausgesprochen werden. Die Themen Datenschutz und Datensicherheit nehmen im Bewusstsein aller Mitarbeiterinnen und Mitarbeiter eine wichtige Rolle ein. Die präventive Einbindung in die jeweiligen Prozesse erleichtert meine Arbeit.

Dank gebührt wiederum dem Referat IT-Sicherheit, das mir mit Rat und Tat zur Seite stand. Hervorzuheben ist das große Engagement von Frau Elisabeth Kunath, die stets ein offenes Ohr für mich hatte.

Ebenso bedanke ich mich sehr herzlich bei meinem Stellvertreter, Herrn Dr. Bernd Appel, der ein wertvoller Ansprech- und Diskussionspartner bei verschiedenen Rechtsfragen war.

Die Datenschutzkontrolle des Kinderkanals obliegt mir gemeinsam mit dem Datenschutzbeauftragten des ZDF, Herr Christoph Bach. Kinderdatenschutz ist und bleibt ein sehr wichtiges Thema, das auch auf ARD-Ebene besonders im Auge behalten werden muss. Gemeinsam mit dem betrieblichen Datenschutzbeauftragten des KiKA, Herrn Jörn Voss, beschäftigen wir uns intensiv mit redaktionellen Fragen im Kontext von Datenschutz. Die Unterstützung von Herrn Voss ist unverzichtbar, und ihm gebührt mein besonderer Dank.

Auch im zweiten Jahr als Beauftragter für den Datenschutz hat sich die mir übertragene Tätigkeit als vielfältig, spannend und lohnend erwiesen. Neben unterschiedliche Themen aus den Bereichen des Beitragszahlerdatenschutzes und des Arbeitnehmerdatenschutzes sowie des bereits beschriebenen Kinderdatenschutzes mussten verschiedene Einzelfragen beleuchtet werden, sodass keine Langeweile aufkommen wollte.

Mein im letzten Bericht bereits beschriebener Eindruck, dass das Thema immer wichtiger wird, hat sich bestätigt. In einer Welt, in der die automatische Datenverarbeitung stets weiter vordringt, werden auch Fragen des Datenschutzes immer drängender. Hier ist gerade der Jurist als Datenschutzbeauftragter besonders gefordert, seine technische Kompetenz weiterzuentwickeln um den Anschluss an den technologischen Fortschritt nicht zu verlieren. Dies zeigt sich insbesondere bei Entwicklungen wie Smart- oder HbbTV, die ernstzunehmende datenschutzrechtliche Hürden aufweisen. Zu diesem Thema darf ich auf ein Kapitel im vorliegenden Bericht verweisen.

Ein brisantes Thema ist auch der Redaktionsdatenschutz. So berichtete das Nachrichtenmagazin „Der Spiegel“ in seiner Ausgabe vom 9. September 2013 darüber, dass die CIA Telekommunikationsdaten eines NDR-Journalisten abgefangen und seine Arbeit und Reisetätigkeiten ausgeforscht haben soll. Ein wesentliches Element einer funktionsfähigen freien Berichterstattung in Presse und Rundfunk ist der Informantenschutz. Journalisten sind auf gegenseitiges Vertrauen angewiesen und dürfen in ihrer Arbeit nicht behindert werden. Im Ergebnis gefährden die bekannt gewordenen Abhör- und Ausspähskandale die demokratische Grundordnung. Freie Presse und Rundfunk sind für die freiheitliche Demokratie schlechthin konstitutiv, wie das Bundesverfassungsgericht immer wieder festgestellt hat. Die Datenschützer von ARD und ZDF haben daher die Politik aufgefordert, das Redaktionsgeheimnis wirksam zu schützen.

Datenschutz dringt als Thema und Herausforderung in praktisch sämtlich Lebensbereiche vor. Oder, wie meine Kollege vom SWR, Herr Prof. Dr. Armin Herb,

es in seinem Tätigkeitsbericht treffend formulierte: Die ruhigen Zeiten im Datenschutz sind vorbei.

2. Aufgaben des Datenschutzbeauftragten

Die Rechtsgrundlagen für den Datenschutzbeauftragten des Mitteldeutschen Rundfunks haben sich im Berichtszeitraum nicht verändert.

Der Beauftragte für den Datenschutz überwacht gemäß § 42 Abs. 2 MDR-Staatsvertrag die Einhaltung der Datenschutzvorschriften dieses Vertrages, des Datenschutzgesetzes des Freistaates Sachsen und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit der Anstalt. Die Bestellung eines Rundfunkdatenschutzbeauftragten folgt dem Gebot der Staatsferne. Er tritt bei der Überwachung des Datenschutzes der Anstalt an die Stelle des Landesbeauftragten für den Datenschutz. Damit wird die Unabhängigkeit von staatlichen Stellen gewahrt. Er untersteht der Dienstaufsicht des Verwaltungsrates und ist in Ausübung seines Amtes ansonsten nur dem Gesetz unterworfen.

Für den redaktionellen Bereich regelt § 40 des MDR-Staatsvertrages, dass bei einer journalistisch-redaktionellen Verarbeitung von Daten nur Datensicherung und Datengeheimnis zu beachten sind. Die Redaktionen dürfen also personenbezogene Daten für eigene journalistische Zwecke verarbeiten. Sie müssen jedoch Geheimnisse schützen, die Privatsphäre achten und Persönlichkeitsrechte wahren. Außerdem muss das Erforderliche dafür getan werden, dass die Daten auch sicher vorgehalten und gespeichert werden.

In enger Zusammenarbeit mit dem Referat IT-Sicherheit und gemeinsam mit den Personalräten obliegt es dem Datenschutzbeauftragten, die technische und organisatorische Ausgestaltung der Datensicherheit zu begleiten und zu überwachen.

Neben der Aufgabe der Überwachung des Datenschutzes sowie der Begleitung von entsprechenden Themen und der Beratung von Mitarbeitern, sind auch Schulungen eine Aufgabe des Datenschutzbeauftragten. Im Berichtsjahr wurde insbesondere in der Abteilung Beitragsservice informiert und geschult, im nächsten Berichtsjahr liegt ein Schwerpunkt bei der Schulung der redaktionellen Bereiche im Kinderkanal.

Der Datenschutz wird gerade angesichts der wachsenden Unübersichtlichkeit des Themas und der vielfältigen Gefährdungen immer wichtiger. Eine Hauptaufgabe des Datenschutzbeauftragten muss daher sein, das Bewusstsein für den Wert von personenbezogenen Daten zu stärken und flankierend für entsprechenden Schutz zu sorgen.

In den folgenden Kapiteln werden die Schwerpunkte meiner Arbeit im Berichtszeitraum beschrieben, die die Vielfältigkeit der Aufgabe illustrieren sollen. Es sei darauf hingewiesen, dass es sich um eine Auswahl der von mir bearbeiteten Vorgänge handelt. Doch zuvor einige Bemerkungen zur Entwicklung des Datenschutzrechts.

3. Entwicklung des Datenschutzrechts

3.1 Europarechtliche Entwicklungen

Wie bereits im letzten Bericht beschrieben, will die Europäische Union das Datenschutzrecht auf eine neue, europäische Grundlage stellen. Im Zuge dieser umfassenden Reform soll eine EU-Datenschutzgrundverordnung in Kraft treten. Dies ist ein Regelwerk, das unmittelbar gegenüber allen Personen gilt und nicht nur den nationalen Gesetzgeber zur Anpassung verpflichtet, wie es etwa eine Richtlinie täte. Dies bedeutet, es wird dem deutschen Gesetzgeber verwehrt sein, bei der Ausgestaltung der rechtlichen Regelungen den Besonderheiten des deutschen Rundfunksystems Rechnung zu tragen. Daher muss schon im Vorfeld alles Wichtige geregelt sein. Für die Datenschützer und die Landesrundfunkanstalten sowie für Medienunternehmen insgesamt ist insbesondere Artikel 80 des Entwurfs von Interesse. Nach diesem ersten Entwurf können Mitgliedsstaaten „für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen oder Ausnahmen vorsehen“. Nach der Fassung des LIBE-Ausschusses des Europäischen Parlaments wird den Mitgliedsstaaten vorgeschrieben, „das Recht auf Schutz der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen“. Damit ist den Landesgesetzgebern die Aufgabe zugewiesen, entsprechende Datenschutzregelungen zu schaffen und sich auch mit der Frage zu beschäftigen, wie die Datenschutz-Aufsichtsbehörde auszugestalten ist, also sich mit Aufgaben der Rundfunkdatenschützer zu befassen.

Der modifizierte Entwurf der EU-Grundverordnung ist am 12. März 2014 in erster Lesung vom EU-Parlament angenommen worden. Damit kann in den sogenannten Trilog mit dem Ministerrat und der Kommission eingetreten werden, bevor es wieder ins EU-Parlament zur Verabschiedung geht.

Ermutigend sind auch nach der ersten Lesung getroffene Änderungen zu Artikel 8 der Grundverordnung, der sich mit dem Datenschutz für Kinder befasst. Mit den dort gefundenen Formulierungen bleibt deutlich mehr Raum für Ange-

bote der öffentlich-rechtlichen Rundfunkanstalten im Netz, insbesondere im Zusammenhang mit der Vermittlung von Medienkompetenz.

Es bleibt insgesamt abzuwarten, wann eine endgültige Verabschiedung der EU-Datenschutzverordnung erfolgen wird.

3. Entwicklung des Datenschutzrechts

3.2 Entwicklung des Bundes- und des Landesrechtes

Im letzten Tätigkeitsbericht hatte ich über die Initiative des Bundes berichtet, ein Arbeitnehmerdatenschutzgesetz zu verabschieden. Im Berichtszeitraum gab es keine weiteren Entscheidungen über dieses Gesetz. Für die Beschäftigten des MDR gilt daher weiterhin § 37 des Sächsischen Datenschutzgesetzes.

§ 39 des MDR-Staatsvertrages sieht vor, dass für den MDR die Vorschriften des Freistaates Sachsen über den Schutz personenbezogener Daten anzuwenden sind, vor allem das Sächsische Datenschutzgesetz (SächsDSG). Anpassungen dieses Gesetzes wurden im Berichtszeitraum nicht vorgenommen.

Auch wurde der Rundfunkbeitragsstaatsvertrag, der verschiedene Vorschriften zum Datenschutz enthält (siehe auch den vorigen Tätigkeitsbericht), im Berichtszeitraum nicht geändert.

4. Datenschutz im MDR

4.1 Vorabkontrolle Employee Self Service

Vor dem Einsatz eines jeden neuen automatisierten Verfahrens, in dem Daten von Beschäftigten des MDR verarbeitet werden, muss der Datenschutzbeauftragte eine sogenannte Vorabkontrolle durchführen. Gemäß § 10 Abs. 4 des Sächsischen Datenschutzgesetzes (SächsDSG) muss dabei geprüft werden, ob die Datenverarbeitung als solche zulässig ist und die Datenverarbeitung den Anforderungen an die Datensicherheit genügt.

Mit einer solchen Aufgabe sah ich mich bei dem Projekt „Employee Self Service“ (ESS) konfrontiert. Der MDR plante, den Mitarbeiterinnen und Mitarbeitern die Möglichkeit zu geben, im Rahmen eines elektronischen Workflows Urlaubsanträge und Abwesenheitsmeldungen papierlos durchzuführen: Hierbei wird mit der SAP-Portaltechnologie eine Weboberfläche angeboten, auf der definierte Abwesenheitsarten beantragt bzw. angezeigt werden können. Hierzu ist eine Vereinbarung zwischen dem MDR und dem Gesamtpersonalrat des MDR geschlossen worden.

Nach der geschlossenen Vereinbarung können die Mitarbeiterinnen und Mitarbeiter selbst ihre Abwesenheiten einsehen sowie direkte und indirekte Vorgesetzte. Art und Umfang der dort hinterlegten Daten sowie der Zeitraum, in der die Abwesenheiten sichtbar sind, sind angemessen gewählt worden und daher datenschutzrechtlich in Ordnung.

Etwas schwieriger war die Frage, die in diesem Zusammenhang hinsichtlich der Sichtbarkeit des Teamkalenders aufgeworfen worden ist. Geplant war, den Teamkalender, der den Überblick über die Abwesenheiten der Mitarbeiter und Mitarbeiterinnen der eigenen Organisationseinheit ermöglicht, ebenfalls für die Mitglieder des jeweiligen Teams freizuschalten. Dies hat der Personalrat abgelehnt. Aus datenschutzrechtlicher Sicht ist es in der Tat nicht erforderlich, auf der gleichen Organisationseinheit die Abwesenheiten der Kolleginnen und Kollegen sehen zu können, da die Verantwortung für eventuelle Vertretungen nicht bei

der Mitarbeiterschaft, sondern beim Vorgesetzten liegt. Eine entsprechende Erlaubnis in der Dienstvereinbarung wäre jedoch nicht zu beanstanden gewesen, da es dem MDR gemeinsam mit dem Personalrat freigestanden hätte, diese Möglichkeit zu eröffnen. Über die Freigabe des Teamkalenders konnte jedoch keine Einigung erzielt werden.

Hinsichtlich der Datensicherheit konnte festgestellt werden, dass die technischen und organisatorischen Maßnahmen ausreichend sind, jedoch fehlt es noch an der Weiterentwicklung des SAP-Sicherheitskonzeptes hinsichtlich der Schnittstelle zum Web. Da es sich zurzeit noch um einen Pilotbetrieb handelt, kann dies toleriert werden, sollte jedoch zum Zeitpunkt des Übergangs in den Regelbetrieb behoben sein.

4. Datenschutz im MDR

4.2 Vorabkontrolle des Planungssystems EVIS für die HA Klangkörper

Im Berichtsjahr hatte ich eine weitere Vorabkontrolle vorzunehmen. Die Hauptabteilung Klangkörper wollte ein neues Planungssystem einführen, mit dem das gesamte Management eines oder mehrerer reisender Ensembles bewerkstelligt werden konnte. Alle organisatorischen Abläufe für Proben, Konzerte, Konzertreihen, Verträge, Reisen etc. sollen mit diesem neuen System „EVIS“ geplant und verwaltet werden. Dabei fallen natürlich auch personenbezogene Daten an, u. a. auch Daten von Kindern des Kinderchors, sodass besonders sorgfältig auf eine ordnungsgemäße Datenverarbeitung geachtet werden musste.

Ausgangspunkt meiner Überlegungen ist stets der § 37 des Sächsischen Datenschutzgesetzes, nach dem Daten von Beschäftigten nur verarbeitet werden dürfen, soweit dies zur Durchführung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist.

In dem Planungssystem „EVIS“ werden Daten der Komponisten, der Dirigenten, der Solisten, der Musiker, der Chormitglieder, der Kinderchormitglieder und deren gesetzlicher Vertreter sowie der Mitarbeiter des Orchestermanagements des MDR gespeichert und verarbeitet. Dies ist erforderlich, um eine sachgerechte Planung und Durchführung der Konzerttätigkeit der Klangkörper zu gewährleisten. An dem Kriterium der Erforderlichkeit mangelte es also bei der Prüfung nicht. In dem Konzept, das meiner Überprüfung zugrunde lag, wird genau beschrieben, welche Daten für welche Zwecke gespeichert und weiterverarbeitet werden sollen. Auch ist die Löschung der Daten in vorschriftsmäßiger Weise geregelt. Der Datenarchivierung für spätere Nutzung auch nach Ausscheiden eines Ensemblemitglieds steht unter dem Vorbehalt einer entsprechenden Einwilligung.

Auch sind Maßnahmen ergriffen worden, die geeignet sind zu gewährleisten, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gesichert ist. Es geht immer darum sicherzustellen, dass die Daten auch dort verbleiben wo sie hingehören, nicht verändert werden und stets zur Verfügung stehen, wenn man sie braucht.

Sowohl auf der datenschutzrechtlichen als auch auf der technischen und organisatorischen Seite der Datenverarbeitungen in dem Planungssystem „EVIS“ konnte ich keine Beanstandungen aussprechen. Insgesamt habe ich daher ein positives Votum abgegeben und eine datenschutzrechtliche Freigabe erklärt.

4. Datenschutz im MDR

4.3 Datenschutz bei Angeboten des MDR auf Drittplattformen

Der MDR verbreitet seine Angebote nicht nur über die drei klassischen Verbreitungswege Fernsehen, Hörfunk und Online, sondern ist auch auf sogenannten Drittplattformen präsent. Beispielhaft aufgezählt seien hier Angebote des MDR auf Facebook und Youtube sowie Twitter. Grundsätzlich können alle digitalen Plattformen benutzt werden, es besteht der Grundsatz der Technologieneutrali-

tät. Damit wird die Strategie verfolgt, den Nutzern die Telemedien des MDR auf den von ihnen bevorzugten Drittplattformen möglichst zielgruppengenau und interessengerecht anzubieten (siehe hierzu die Leitlinien des MDR für Telemedizinangebote des MDR auf Plattformen Dritter; Stand 10. Juni 2014).

Auch bei seinen eigenen Onlineangeboten sorgt der MDR für korrekten Datenschutz. In seiner Datenschutzerklärung, die von allen Seiten zu erreichen ist, wird genau erläutert, welche Daten gespeichert und wofür Daten benötigt werden. Außerdem ist vollkommen klar, dass eine Weitergabe an Dritte gerade zu werblicher oder anderer kommerzieller Nutzung auf gar keinen Fall stattfindet.

Diesen Standard kann der MDR bei Drittplattformen natürlich nicht garantieren. Wer bei Facebook unterwegs ist und dort ein Angebot des MDR anschaut oder auch kommentiert, begibt sich in die „Hände“ dieser Plattform. Facebook sammelt Daten und speichert sie auch in den USA. Zudem werden möglicherweise Persönlichkeitsprofile erstellt und für zielgerichtete Werbung benutzt. Dies muss jeder Nutzer wissen, der auf einer solchen Drittplattform Angebote nutzt. Die Verantwortung des MDR, und damit von mir als Datenschützer, besteht an dieser Stelle darin, dafür zu sorgen, dass der Nutzer aufgeklärt ist. Daher muss bei jedem Angebot des MDR auf Drittplattformen deutlich darauf hingewiesen werden, dass der Bereich des vom MDR verantworteten Onlineumfeldes verlassen wird und der Datenschutz möglicherweise nicht mehr den deutschen bzw. europäischen Standards entspricht. Grundsätzlich gehe ich von einem mündigen Nutzer aus, aber ein Hinweis darf trotzdem nicht fehlen. An diesem Beispiel wird deutlich, dass Datenschutz nicht immer die gleiche Zielrichtung verfolgt wie journalistische Zwecke. Daher müssen, wie die genannten Beispiele zeigen, Kompromisse gefunden werden, die sowohl der freien Berichterstattung als auch dem Datenschutz Rechnung tragen.

4. Datenschutz im MDR

4.4 Aufbewahrung von Zuschauerpost

Viele Menschen wenden sich schriftlich an den MDR. Die Zuschauerredaktion freut sich sehr über Reaktionen auf Sendungen, über Kritik, Anregungen und andere Anfragen. Dabei fallen natürlich personenbezogene Daten wie insbesondere Name und Adresse sowie ggf. E-Mail-Adresse an. Der Datenschutzbeauftragte fragt sich hierbei, müssen diese Daten aufbewahrt werden und wenn ja, wie lange? Jetzt könnte man einwenden, dass diese Daten freiwillig von den Zuschauerinnen und Zuschauern zur Verfügung gestellt werden und daher keine Begrenzungen gelten. Außerdem könnte man argumentieren, dass die Zuhörer und Zuschauer erwarten, dass sich der MDR an sie erinnert, wenn sie mehrfach schreiben oder wenn sie Bezug auf eine Anmerkung nehmen, die vielleicht schon Jahre zuvor gemacht worden ist.

Dies sind durchaus sachliche Gründe, die auch nachvollziehbar sind. Dennoch müssen zwei Grundsätze des Datenschutzes, die „Datensparsamkeit“ und die „Datenvermeidung“ bei der Aufbewahrung von Zuschauerdaten beachtet werden: Es dürfen also nur diejenigen Daten aufbewahrt werden, die tatsächlich benötigt werden, und auch nur für einen möglichst kurzen Zeitraum.

Dieses Thema wurde auch im Kollegenkreis der Datenschützer von ARD und ZDF diskutiert. Für den MDR bin ich in Absprache mit der Zuschauerredaktion zu dem Ergebnis gekommen, dass keine Notwendigkeit gesehen wird, Zuschauerzusendungen länger als ein Jahr aufzubewahren. Auch eingehende E-Mails und Antworten darauf sollten nach spätestens einem Jahr gelöscht werden, wenn nicht einiges dafür spricht, dies auch früher zu tun. Ich habe die Zuschauerredaktion auch gebeten, ihre Archivbestände zu „durchforsten“ und ggf. Altbestände einer datenschutzgerechten Löschung, d. h. der Aktenvernichtung zuzuführen. Ich glaube, man kann jedem Zuhörer oder Zuschauer, der sich mehrfach an die Zuschauerredaktion wendet, sehr gut erklären, dass man seine vorherigen Schreiben nach einem Jahr vernichtet hat, um keine unnötigen Datenbestände anzuhäufen. Die meisten Menschen werden Verständnis für die Belange des Daten-

schutzes aufbringen, denn die Löschung der Bestände erfolgt ja in ihrem Interesse.

4. Datenschutz im MDR

4.5 HbbTV und Datenschutz

Die moderne Fernsehwelt ändert sich. Moderne Geräte bieten neben dem klassischen Fernsehempfang auch die Möglichkeit, Internetdienste aufzurufen. Dem Zuschauer ist es damit möglich, parallel zum laufenden Fernsehprogramm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen. Dies ist mit sogenannten Smart-TVs möglich, der Standard, der beim öffentlich-rechtlichen Rundfunk zurzeit zur Anwendung kommt, nennt sich HbbTV (Hybrid Broadcasting Broadband TV). Kurz gesagt, es handelt sich um die Verschmelzung von Fernsehen und Internet.

Immer wenn es um das Internet geht, wird der Datenschützer deswegen hellhörig, weil die sogenannte IP (Internetprotokoll)-Adresse übertragen werden muss, um Inhalte aus dem Internet anzeigen zu können. Nach herrschender Auffassung ist diese IP-Adresse ein personenbezogenes Datum, sodass der Datenschutz Anwendung findet.

Der Kreis der staatlichen Aufsichtsbehörden hat sich ebenso wie die Rundfunkdatenschützer dieses Themas angenommen, und es wurde im Mai 2014 eine gemeinsame Position verabschiedet. Die zentrale Forderung ist, dass die anonyme Fernsehnutzung auch bei der Smart-TV-Nutzung gewährleistet sein muss. Es muss sichergestellt werden, dass eine Profilbildung über das individuelle Fernsehverhalten ohne Information und ausdrückliche Einwilligung der Zuschauer verhindert wird. Wenn tatsächlich der Zugang zum Internet geöffnet wird, muss dafür Sorge getragen werden, dass alle gesetzlichen Vorschriften eingehalten werden und die personenbezogenen Daten (in unserem Fall die IP-Adresse) nur dann verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich sein könnte. Wichtig ist für Datenschützer auch

immer, dass umfassend informiert und transparent gemacht wird, was mit den Daten passiert und wofür sie tatsächlich erhoben werden. Auch der öffentlich-rechtliche Rundfunk hat natürlich ein Interesse daran, das Nutzerverhalten zu analysieren – natürlich nur anonym – um seine Angebote den Nutzervorlieben anzupassen.

Bekanntlich steckt der Teufel im Detail. Die Datenschützer waren und sind an dieser Stelle aufgefordert, auch technische Feinheiten zu beachten und die Konsequenzen daraus zu bedenken. So ist es beispielsweise möglich, die Internetverbindung im Hintergrund des Fernsehsignals mitzusenden und damit schon einen Datenaustausch vorzunehmen, bevor der Nutzer sich überhaupt entschieden hat, das Internet tatsächlich parallel zum Fernsehen zu nutzen. Hier muss intensiv aufgeklärt werden, der Nutzer muss überdies in die Lage versetzt werden, diesen Dienst auch abzustellen. Ihm muss klar sein, wann eine Verbindung zum Internet besteht und was dann mit seinen Daten passiert. Es ist auch zu beachten, was die Endgeräte technisch vermögen und wie man die Forderungen des Datenschutzes am besten umsetzt, ohne gleich das ganze Angebot schwerfällig und kaum noch nutzbar zu gestalten. Insgesamt sind wir auf einem guten Weg: Techniker, Entwickler und Datenschützer tauschen sich aus und suchen gemeinsam nach Lösungen. Die technischen Möglichkeiten und die damit verbundenen Anwendungen stellen uns vor Herausforderungen, die auch in den nächsten Jahren den öffentlich-rechtlichen Rundfunk und die Rundfunkdatenschützer beschäftigen werden.

4. Datenschutz im MDR

4.6 Rentenalter von freien Mitarbeitern

Die Abteilung Honorare und Lizenzen wollte von mir wissen, ob sie das Datum „Eintritt in das Rentenalter“ bei freien Mitarbeitern im Rahmen eines SAP-Berichtes verarbeiten dürfe. Zweck dieser Datenverarbeitung ist, dass die Bereiche rechtzeitig über die Veränderung des gesetzlichen Status der freien Mitarbeiter informiert sind. Die einsetzenden Bereiche möchten wissen, wie lange ein

freier Mitarbeiter noch zur Verfügung steht und ob entsprechende Perspektivgespräche geführt werden müssen. Auch müssen Mitteilungsfristen eingehalten werden, wenn eine freie Tätigkeit beendet werden soll. Schließlich soll ein arbeitsrechtliche Risiko gesteuert werden: Bei freien Mitarbeitern, die nicht programmgestaltend tätig sind und keinen Honorarrahmenvertrag haben, besteht das Risiko, dass sie sich nach Erreichen des Renteneintrittsalters mithilfe einer Statusklage als feste Mitarbeiter einklagen könnten und damit ohne festen Beendigungszeitpunkt beschäftigt werden müssten.

Auf den ersten Blick erscheint diese Frage etwas seltsam: Die Geburtsdaten von festen und freien Mitarbeitern sind im MDR natürlich bekannt, sodass eine Berechnung des Renteneintrittsalters problemlos möglich ist. Entscheidend ist aber hier, dass die (Weiter-)Verarbeitung von solchen personenbezogenen Daten (auch wenn sie bekannt sind) davon abhängig ist, ob diese zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses erforderlich sind.

Zunächst habe ich mir die Tarifverträge angeschaut. Der Bestandsschutztarifvertrag sieht vor, dass der Vertrag zwischen dem MDR und der freien Mitarbeiterin endet, ohne dass es einer Kündigung bedarf, mit dem Zeitpunkt, der gesetzlich als Zeitpunkt für einen Bezug von Regelaltersrente als Vollrente ohne Abschläge bestimmt ist. Wenn der freie Mitarbeiter also unter den Bestandsschutztarifvertrag fällt, muss bekannt sein, wann er das Renteneintrittsalter erreicht, da damit automatisch seine Beschäftigung endet. Damit liegt eine Grundlage für die Datenverarbeitung vor, insofern gibt es hier keine Probleme.

Für alle anderen freien Mitarbeiter gilt, dass der MDR relativ frei entscheiden kann – unter Berücksichtigung der tarifvertraglichen Vorgaben –, ob ein freier Mitarbeiter weiterbeschäftigt werden soll oder nicht. Hat der MDR sich also entschieden, einen freien Mitarbeiter mit Erreichen des Rentenalters nicht mehr zu beschäftigen, so kann er dies tun, braucht dafür aber auch das entsprechende Datum. Ebenso hat der MDR ein legitimes Interesse daran, arbeitsrechtliche Risiken zu minimieren und darf die dafür notwendigen Daten benutzen. Bei der

Abwägung ist auch nicht verkannt worden, dass das Erreichen des Renteneintrittsalters kein sensibles Datum ist, da das Alter der Beschäftigten beim MDR bekannt ist. Insofern konnte ich für die Anfrage „grünes Licht“ geben. Ein entsprechender SAP-Bericht ist damit zulässig.

4. Datenschutz im MDR

4.7 Sichtbarkeit von Druckaufträgen

Durch den Personalrat Zentrale wurde ich auf einen Umstand hingewiesen, der datenschutzrechtlich nicht ganz unproblematisch ist: Wenn sich Druckaufträge in der Warteschleife befinden, so ist es jedem Nutzer möglich, seine noch nicht abgearbeiteten Druckaufträge anzusehen und gegebenenfalls zu löschen und den Druckauftrag neu zu starten. Durch eine Fehlfunktion im System kam es zu einer Stauung verschiedener Druckaufträge bei dem zentralen Druckerserver, sodass auch die Druckaufträge anderer Mitarbeiterinnen und Mitarbeiter zumindest kurzfristig sichtbar waren. Dies ist datenschutzrechtlich deswegen bemerkenswert, weil zum einen sichtbar ist, welcher Mitarbeiter welche Dokumente druckt und zum anderen die Möglichkeit besteht, dass auch personalrelevante Dokumente gedruckt werden, die schon aufgrund der Bezeichnung als kritisch zu bewerten sind. Anders ausgedrückt: Was jemand anderes druckt, geht erst einmal die anderen Mitarbeiterinnen und Mitarbeiter nichts an und muss vertraulich behandelt werden.

Seitens der Betriebsdirektion wurde ich darüber informiert, dass es keine technische Möglichkeit gibt, Informationen in der Anzeige der Druckerwarteschlange auszublenden oder zu anonymisieren. Die Firma Microsoft konnte hierzu keine Lösung anbieten. Gemeinsam mit Vertretern der Betriebsdirektion und des Personalrats Zentrale wurde daher weiter überlegt, wie dieses Problem zu lösen sein könnte. Schließlich wurde klar, dass mit dem Einsatz des neuen Serverbetriebssystem von Microsoft (MS-Server2012) bei Printservern das bestehende Problem gelöst werden kann. Bei der Anzeige von „Druckerwarteschlangen“ werden die Dateinamen nur noch für eigene Druckaufträge angezeigt, die an-

derer Nutzer nicht. Damit ist zwar auch sichtbar, dass jemand anderes druckt, jedoch nicht mehr, welche Dokumente ausgedruckt werden sollen. Dies ist aus datenschutzrechtlicher Sicht akzeptabel. Eine Realisierung der Lösung soll noch in 2014 erfolgen. Bislang habe ich noch keine Informationen darüber erhalten, wann die technische Umstellung tatsächlich realisiert werden kann. Ich habe allerdings auf eine möglichst schnelle Umsetzung gedrängt.

4. Datenschutz im MDR

4.8 Programmvergabebericht

Der MDR gibt einen Programmvergabebericht heraus. Informiert werden soll über Fernsehproduktionen, mit deren Fertigung der MDR Produzenten im jeweiligen Jahr unmittelbar beauftragt hat. Adressaten dieses Berichtes sind die Gremien, die Politik sowie die Produzentenallianz. Eine Veröffentlichung des Berichtes im Internet ist auch denkbar. Im Programmvergabebericht soll als Anlage eine Liste derjenigen Produktionsfirmen beigefügt werden, an die der MDR im jeweiligen Jahr Aufträge vergeben hat. Die Firmen und Produzenten sollen dort namentlich aufgeführt werden. Die Frage, ob ein solches Vorgehen datenschutzrechtlich zulässig ist, wurde an mich herangetragen.

Juristische Personen besitzen kein Recht auf informationelle Selbstbestimmung, dies ist den natürlichen Personen vorbehalten. Daher habe ich keine datenschutzrechtlichen Bedenken angemeldet, falls dort Produktionsfirmen aufgeführt werden sollen. Soweit es sich allerdings um Einzelproduzenten und damit (auch) Privatpersonen handelt, mit denen Produktionsverträge geschlossen wurden, halte ich eine explizite und auch schriftliche Einwilligung in die Veröffentlichung für unabdingbar. Nur wenn sie ihre Erlaubnis dafür erteilt haben, namentlich im Produzentenbericht aufgeführt zu werden, kann dies datenschutzrechtlich auf sicheren Füßen stehen. Weiterhin habe ich darauf hingewiesen, dass in die Auftragsproduktionsverträge eine solche Einwilligung integriert werden kann, jedoch ist diese Einwilligung im äußeren Erscheinungsbild des Vertrages hervorzuheben. Die vorgesehene Einwilligungserklärung muss also optisch

auffällig gestaltet sein. Auch sollte sie idealerweise im Rahmen des Vertrages gesondert unterschrieben werden. Dies ist aber nicht unbedingt notwendig, wenn klar wird, dass mit der einzigen Unterschrift unter den Vertrag auch die Einwilligung in die Datennutzung im Rahmen des Programmvergabeberichtes erklärt wird.

5. Datenschutz beim KiKA

5.1 Unterarbeitsgruppe Datenschutz bei Kindern und Jugendlichen

In meinem letzten Tätigkeitsbericht habe ich über das Thema Kinderdatenschutz beim Kinderkanal ausführlich berichtet. Insbesondere die Frage, wie mit Daten umzugehen ist, die Kinder beim Besuch von Onlineangeboten des KiKA hinterlassen, hat mich und Herrn Jörn Voss, den betrieblichen Datenschutzbeauftragten des KiKA, eingehend beschäftigt. Die Bemühungen kreisen stets um das Ziel, Kriterien zu entwickeln, die eine Bewertung der Angebote als pädagogisch sinnvoll und datenschutzrechtlich unbedenklich ermöglichen und die Beantwortung der Frage, inwieweit es Kindern schon vor Erreichen der Volljährigkeit möglich ist, die Folgen von Datenpreisgabe und den Umgang mit dem Internet angemessen einzuschätzen.

Im Zuge dieser Bemühungen habe ich eine Sitzung der Jugendschutzbeauftragten von ARD und ZDF besucht, um dort für das Thema zu werben und mich der Unterstützung der Jugendschützer zu versichern. Dort wurde ich verwiesen auf das Internationale Zentralinstitut für Jugend- und Bildungsfernsehen (IZI). Im Dezember 2013 fand dort eine Beratung zu dem Thema statt, wie Kinder das Internet nutzen und welche Einsichtsfähigkeit in ihr Tun bereits besteht. Hier konnten erste Altersabstufungen getroffen werden. Außerdem konnte ich lernen, dass der spielerische Weg in die Onlinewelt, auf dem Kinder in leichter Weise mit den Problemen konfrontiert werden und dabei mit Spielen oder Quizen ihre Fähigkeiten hinsichtlich der Einsicht in die Gefahren und Möglichkeiten der Datenpreisgabe im Internet verbessern können, ein guter Ansatz ist.

Die Frage bleibt jedoch nach der Klärung der Stufen der Einsichtsfähigkeit bei Kindern und Teenagern. Ebenso muss die Frage beantwortet werden, welche Art und Tiefe der Einsichtsfähigkeit es bei der Nutzung der verschiedenen Angebote braucht.

Datenschutzvorgaben bei Internetseiten von Kindern standardisieren den Umgang mit den gesetzlichen Vorgaben und dienen den Redaktionen bei zukünftigen Angeboten und Formaten als Orientierung. Ziel ist es, eine Datenschutzkultur umzusetzen, die dem öffentlich-rechtlichen Rundfunk sowohl höhere und damit rechtssicherere Freiheitsgrade in den Angeboten erlaubt, als auch die Möglichkeit bietet, sich von den Mitbewerbern im Hinblick auf Qualität und Engagement deutlich abzuheben.

Dieses Thema wurde auch mit der Programmgeschäftsführung des KiKA besprochen und hat dort ermutigende Resonanz gefunden. Ein entsprechendes Forschungsvorhaben zur eingehenden Untersuchung von Nutzerverhalten und Einsichtsfähigkeit wird zurzeit noch nicht umgesetzt, jedoch wurde zugesagt, bei der Datenerhebung von Kindern und Jugendlichen besonders sparsam vorzugehen und flankierend zu den einzelnen Angeboten dem Thema Datenschutz besondere Aufmerksamkeit zu widmen. Es wird sich zeigen, inwieweit die Frage nach den Stufen der Einsichtsfähigkeit von Kindern und Jugendlichen von ARD und ZDF auch auf wissenschaftlichem Weg weiter verfolgt wird. Ich beabsichtige jedenfalls, dieses Thema weiter voranzutreiben, damit es nicht bei den starren Regeln bleibt.

Auch neue Überlegungen und Vorschläge zur EU-Grundverordnung sind insoweit ermutigend, dass die Einwilligung der Eltern jedenfalls nicht mehr unbedingt erforderlich ist im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar dem Kind angeboten werden. Hier öffnen sich zukunftsweisende Felder auch für den öffentlich-rechtlichen Rundfunk.

Es bleibt also ein Thema, das ich weiterhin mit besonderer Aufmerksamkeit beobachten werde.

5. Datenschutz beim KiKA

5.2 Klage wegen KiKA-Gewinnspiel

Unter Ziffer 5.2 hatte ich im vergangenen Tätigkeitsbericht eine Klage des Bundesverbandes der Verbraucherzentralen und Verbraucherverbände gegen den MDR thematisiert. Der Bundesverband warf dem MDR vor, dass Kinder bei der Anmeldung zu einem Gewinnspiel aufgefordert werden, neben E-Mail-Adresse auch Vor- und Nachname, Alter und Wohnort anzugeben. Es wurde die Auffassung vertreten, dass ein Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb damit zu begründen sei, dass dem Grundsatz der Datenvermeidung und der Datensparsamkeit nicht genügt werde. Der MDR und der KiKA hatten mit dem pädagogischen Konzept argumentiert, das auch mit Hilfe der persönlichen Ansprache darauf ausgerichtet ist, die Kinder in allen Lebenssituationen ernst zu nehmen.

Die Klage ist vom Landgericht Leipzig abgewiesen worden und auch die Berufung beim Oberlandesgericht Dresden hatte keinen Erfolg, worüber ich ausführlich berichtet habe. Eine Revision wurde nicht zugelassen, jedoch haben die Verbraucherzentralen eine Nichtzulassungsbeschwerde beim Bundesgerichtshof in Karlsruhe eingelegt.

Mit Beschluss des Bundesgerichtshofes vom 13. März 2014 ist die Beschwerde gegen die Nichtzulassung der Revision gegen das Urteil des Oberlandesgerichtes Dresden abgewiesen worden. Begründet wurde diese Abweisung kurz und knapp allein damit, dass dieses Rechtsmittel mangels Erreichen der dafür erforderlichen Schwelle von über 20.000 € bereits nicht statthaft sei. Das klageabweisende Urteil des Landgerichts Leipzig vom 17. Oktober 2012 ist damit rechtskräftig. Die Klage gegen den MDR wegen des KiKA-Gewinnspiels hatte damit endgültig keinen Erfolg.

6. Datenschutz beim Beitragsservice

6.1 Datenschutz im Zusammenhang mit dem Rundfunkbeitrag

Die Überwachung des Datenschutzes bei der Verarbeitung der Rundfunkteilnehmerdaten obliegt dem Datenschutzbeauftragten der jeweils zuständigen Landesrundfunkanstalt. In diesem Zusammenhang fallen verschiedene Eingaben und Auskunftersuchen von Rundfunkteilnehmerinnen und Rundfunkteilnehmern an. Grundsätzlich werden diese, sofern keine Besonderheiten ersichtlich sind, von der Stelle beantwortet, an die die Anfrage gerichtet ist. Wenn die Anfragen direkt beim MDR, meistens in der Abteilung Rundfunkbeitrag, eingehen, werden sie also dort auch beantwortet. Wenn es datenschutzrechtlich schwierige Fragen gibt, werde ich hinzugezogen, ansonsten wird Auskunft über die gespeicherten Daten gegeben und erläutert, auf welcher Rechtsgrundlage (Rundfunkbeitragsstaatsvertrag) die Daten erhoben und verarbeitet werden und auf die strenge Zweckbindung hingewiesen, nach der die Daten ausschließlich zum Zwecke des Beitragseinzugs verwendet werden dürfen.

Im Berichtszeitraum haben mich persönlich 21 Anfragen erreicht, die jedoch auch hauptsächlich von der Abteilung Beitragsservice beantwortet werden konnten, denn dort werden die entsprechenden Daten vorgehalten.

Beim Beitragsservice von ARD, ZDF und Deutschlandradio mit Sitz in Köln ist eine betriebliche Datenschutzbeauftragte tätig, deren Aufgaben sich nach den Bestimmungen des Bundesdatenschutzgesetzes richten, und die eng mit dem nach Landesrecht für die jeweilige Rundfunkanstalt zuständigen Datenschutzbeauftragten zusammenarbeitet. Sie erstattet regelmäßig Bericht über die Situation des Datenschutzes bei dieser Gemeinschaftseinrichtung. Datenschutzrechtliche Vorfälle, die einer gesonderten Aufmerksamkeit der Datenschutzbeauftragten der Landesrundfunkanstalten bedurft hätten, gab es im Berichtszeitraum nicht.

6. Datenschutz beim Beitragsservice

6.2 Schulung der Regionalberater

Am 14. Mai 2014 fand eine Schulung der Regionalberater zum Datenschutz statt. Die Aufgabe der Regionalberater besteht darin, als Ansprechpartner für Fragen des Rundfunkbeitrages und zur Sachverhaltsklärung bei Unternehmen vor Ort zu fungieren. Im Zuge dessen gehen sie mit personenbezogenen Daten um. Es handelt sich hierbei um Daten von Beitragszahlern, die einer besonderen Zweckbindung, nämlich ausschließlich dem Beitragseinzug dienend, unterliegen und damit als externe Daten unserer „Kunden“ besonders schutzwürdig sind.

Zur Erfüllung ihrer Aufgaben erhalten die Regionalberater vom MDR daher Daten von potenziellen Beitragsschuldnern, die folglich im Auftrag des MDR durch die Regionalberater verarbeitet werden. Die damit erforderlichen Auftragsdatenverarbeitungsverträge sind geschlossen worden und normieren einige Pflichten hinsichtlich der Datenvorhaltung und Datenverarbeitung.

In meinem Vortrag habe ich zunächst die Grundlagen des Datenschutzes erläutert. Nach der Definition von personenbezogenen Daten und Darstellung der rechtlichen Grundlagen bin ich auf die gesetzlichen Vorgaben des Sächsischen Datenschutzgesetzes, des Rundfunkbeitragsstaatsvertrages und die verschiedenen Ausprägungen der Datenverarbeitung eingegangen. Wichtig ist vor allen Dingen, dass keine Daten auf Vorrat gespeichert werden und sie für keine anderen Zwecke als für den Rundfunkbeitragseinzug genutzt werden. Ich habe die Regionalberater darüber hinaus auf ihre vertraglichen und gesetzlichen Pflichten hingewiesen und gemeinsam mit Herrn Heiko Lehmann vom Referat IT-Sicherheit auf die Umsetzung der Vorgaben zur sicheren Datenvorhaltung und sicheren Datenverarbeitung hingewiesen. Besonders wichtig ist, dass die Vertraulichkeit gewahrt wird, dass die Daten nicht verändert oder verfälscht werden und dass sie jederzeit für die vorgesehenen Zwecke verfügbar sind.

Im weiteren Verlauf der Schulung wurde geklärt, inwieweit die Regionalbeauftragten die Vorgaben aus dem Vertrag und aus den Gesetzen umgesetzt haben. Hier konnten einige wichtige Hinweise gegeben werden, es wurden überdies gewisse Defizite aufgedeckt.

Als Fazit lässt sich sagen, dass durch die Vermittlung von Informationen und die Vertiefung von bereits vorhandenem Wissen ein Beitrag zur sicheren Verarbeitung von Beitragszahler-Daten geleistet werden konnte.

7. Externe Prüfungen

7.1 Informationsverarbeitungszentrum (IVZ)

Beim Rundfunk Berlin Brandenburg (RBB) wird als Gemeinschaftseinrichtung des Deutschlandradios, des MDR, des NDR, des RB, des RBB, des SR und des WDR das Informationszentrum (IVZ) betrieben. Dort werden zentral verschiedene Aufgaben der elektronischen Datenverarbeitung für die beteiligten Anstalten abgewickelt. Am 28. November 2013 fand das jährliche Treffen der beteiligten Datenschützer im IVZ in Berlin statt. Ausführlich wurde seitens des IVZ über datenschutzrechtliche Fragen und Entwicklungen informiert. Es gab keinerlei Probleme, die ein Tätigwerden der Datenschutzbeauftragten erfordert hätte.

7. Externe Prüfungen

7.2 IVZ-Verwaltungsvereinbarung

Bereits vor einigen Jahren war seitens der Datenschutzbeauftragten des RBB, Frau Anke Naujock, und der Leiterin des Ressorts IT-Sicherheit des MDR, Frau Elisabeth Kunath, die Initiative gestartet worden, die IVZ-Verwaltungsvereinbarung zwischen den beteiligten Anstalten um ergänzende Regelungen zu Datenschutz, Informationssicherheit und Vertraulichkeit zu erweitern. Im Juni 2014 hatte ich Gelegenheit, an diesem Text mitzuarbeiten. Aufgrund der Tatsache, dass beim IVZ vielerlei auch sensible Daten der Rundfunkanstalten verarbeitet werden, ist es sinnvoll, dem Datenschutz eine höhere Bedeu-

tung durch die Integration in die Verwaltungsvereinbarung einzuräumen. Es sind Regelungen zu konkreten technischen und organisatorischen Maßnahmen nach Maßgabe der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik und bestimmte Entscheidungs- und Meldungsabläufe vorgesehen.

Der Verwaltungsrat des IVZ hat der Erweiterung der Verwaltungsvereinbarung am 11. September 2014 zugestimmt.

8. Zusammenarbeit im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) ist ein gemeinsames Gremium der Rundfunkdatenschutzbeauftragten dessen Ziel es ist, Erfahrungen und Meinungen zu datenschutzrechtlichen Problemen in den Rundfunkanstalten auszutauschen und den Datenschutz beim Rundfunkbeitragszugang sowie bei Gemeinschaftsprojekten zu koordinieren. Darüber hinaus begleitet der Arbeitskreis auch die gesetzgeberischen Aktivitäten, sofern Fragen des Datenschutzes und der Datensicherheit im Rundfunk betroffen sind.

Die Datenschutzbeauftragten treffen sich zwei Mal jährlich, im Berichtszeitraum am 24./25. Oktober 2013 und am 03./04. April 2014.

Im AK DSB waren im Berichtszeitraum insbesondere folgende Themen Gegenstand der Beratungen und des Austausches:

- Beobachtung der Entwicklung der datenschutzrechtlichen Gesetzgebung und Rechtsprechung auf europäischer und bundesdeutscher Ebene
- Sicherstellung des Datenschutzes in den redaktionellen Bereichen
- Anforderungen an den Kinderdatenschutz bei Onlineangeboten
- Wirksamer Datenschutz beim Rundfunkbeitragszugang

- HbbTV/Smart-TV

Wie bereits im letzten Bericht ausgeführt, hat sich der Kreis der Datenschutzbeauftragten als sehr rühriges und kollegiales Gremium erwiesen. Sowohl die eigenen Themen, die in den einzelnen Häusern Gegenstand der Beratungen sind, als auch übergreifende, d. h. alle Anstalten betreffenden Themen werden lebhaft diskutiert, um sachgerechte Lösungen für alle Beteiligten zu finden. Besonders Erwähnung finden sollte die Tatsache, dass bei der Befassung der Frage des Datenschutzes für Smart-TV/HbbTV eine gemeinsame Position mit den staatlichen Datenschützern („Düsseldorfer Kreis“) gefunden werden konnte. Diese erfolgreiche Zusammenarbeit, so die Meinung des AK DSB, sollte fortgesetzt werden.

9. Schlussbemerkungen

Das zweite Jahr meiner Amtszeit hat gezeigt, dass Datenschutz immer wichtiger wird, die allgegenwärtigen Prognosen also richtig sind. Man kann in jedem Bereich des MDR „fündig“ werden, wenn es um Datenschutzthemen geht. Daher ist es umso wichtiger, Aufklärung zu betreiben und für Fragen ein offenes Ohr zu haben.

Die komplexer werdende Technik birgt dabei eine besonders große Herausforderung und erneut gilt mein besonderer Dank dem Referat IT-Sicherheit, dass bei den vielfältigen technischen Themen den Überblick behält und mir als Datenschutzbeauftragten eine große Hilfe ist.

Ich bin der festen Überzeugung, dass der MDR im Bereich Datenschutz bestens aufgestellt ist. Vieles kann natürlich noch verbessert werden, sodass meine Aufgabe ganz sicher nicht langweilig werden wird.

Mein Dank gilt dem gesamten Haus und den engagierten Mitarbeitern, mit denen eine Zusammenarbeit stets fruchtbar und erfolgreich war. Ich bin sicher,

dass der nächste Bericht, den ich in zwei Jahren abzugeben habe, ein ebenso positives Bild vom Stand des Datenschutzes beim MDR zeigen wird.

10. Anhang

10.1 §§ 39 bis 42 MDR-Staatsvertrag

§ 39 Geltung von Datenschutzvorschriften

Soweit nachfolgend nichts anderes bestimmt ist, sind für den MDR die Vorschriften des Freistaates Sachsen über den Schutz personenbezogener Daten anzuwenden.

§ 40 Datenverarbeitung für journalistisch-redaktionelle Zwecke

Werden personenbezogene Daten durch die Rundfunkanstalt zu journalistisch-redaktionellen Zwecken verarbeitet, gelten nur die für die Datensicherung und das Datengeheimnis maßgeblichen Vorschriften des Datenschutzgesetzes.

§ 41 Rechte der Betroffenen

(1) Führt die journalistisch-redaktionelle Verwendung personenbezogener Daten zu Gegendarstellungen der Betroffenen, so ist ein Hinweis darauf zu den gespeicherten Daten zu nehmen. Dieser und die Gegendarstellung sind für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(2) Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, so kann der Betroffene Auskunft über die der Berichterstattung zugrundeliegenden zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmanns von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Der Betroffene kann die Berichtigung unrichtiger Daten, sofern deren Unrichtigkeit feststeht, oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen.

§ 42 Beauftragter für den Datenschutz in der Rundfunkanstalt

(1) Der Verwaltungsrat bestellt für die Dauer von vier Jahren auf Vorschlag des Intendanten einen Beauftragten für den Datenschutz, der an die Stelle des Landesbeauftragten für den Datenschutz tritt. Wiederbestellungen sind zulässig. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz in der Rundfunkanstalt überwacht die Einhaltung der Datenschutzvorschriften dieses Vertrages, des Datenschutzgesetzes des Freistaates Sachsen und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit der Anstalt. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er der Dienstaufsicht des Verwaltungsrates.

(3) Jeder kann sich an den Beauftragten für den Datenschutz in der Rundfunkanstalt wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch die Rundfunkanstalt in seinen Rechten verletzt worden zu sein.

(4) Stellt der Beauftragte für den Datenschutz in der Rundfunkanstalt Verstöße gegen die Vorschriften dieses Vertrages oder anderer Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so fordert er ihre Behebung innerhalb angemessener Frist.

(5) Wird ein Verstoß nicht behoben, so teilt er dies dem Intendanten mit und fordert innerhalb angemessener Frist geeignete Maßnahmen (Beanstandung). Mit der Beanstandung kann der Beauftragte für den Datenschutz in der Rundfunkanstalt Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(6) Der Intendant unterrichtet den Beauftragten für den Datenschutz in der Rundfunkanstalt über die von ihm getroffenen Maßnahmen.

(7) Der Beauftragte für den Datenschutz in der Rundfunkanstalt kann sich jederzeit an den Verwaltungsrat wenden (Anrufungsrecht).

(8) Der Beauftragte für den Datenschutz der Rundfunkanstalt erstattet den Organen der Rundfunkanstalt alle zwei Jahre einen Bericht über seine Tätigkeit.

10. Anhang

10.2 Artikel 28 und 29 EG-Richtlinie 95/46 vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Artikel 28 Kontrollstelle

(1) Die Mitgliedsstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedsstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

(2) Die Mitgliedsstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.

(3) Jede Kontrollstelle verfügt insbesondere über:

- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrages erforderlichen Informationen;

- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;

- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie. Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.

(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde. Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat.

(5) Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedsstaates für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig, unabhängig

vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedsstaates um die Ausübung ihrer Befugnisse ersucht werden. Die Kontrollstellen sorgen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen.

(7) Die Mitgliedsstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.

Artikel 29 Datenschutzgruppe

(1) Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt (nachstehend "Gruppe" genannt). Die Gruppe ist unabhängig und hat beratende Funktion.

(2) Die Gruppe besteht aus je einem Vertreter, der von den einzelnen Mitgliedsstaaten bestimmten Kontrollstellen und einem Vertreter der Stelle bzw. der Stellen, die für die Institutionen und Organe der Gemeinschaft eingerichtet sind sowie einem Vertreter der Kommission. Jedes Mitglied der Gruppe wird von der Institution, der Stelle oder den Stellen, die es vertritt, benannt. Hat ein Mitgliedsstaat mehrere Kontrollstellen bestimmt, so ernennen diese einen gemeinsamen Vertreter. Gleiches gilt für die Stellen, die für die Institutionen und die Organe der Gemeinschaft eingerichtet sind.

(3) Die Gruppe beschließt mit der einfachen Mehrheit der Vertreter der Kontrollstellen.

(4) Die Gruppe wählt ihren Vorsitzenden. Die Dauer der Amtszeit des Vorsitzenden beträgt zwei Jahre. Wiederwahl ist möglich.

(5) Die Sekretariatsgeschäfte der Gruppe werden von der Kommission wahrgenommen.

(6) Die Gruppe gibt sich eine Geschäftsordnung.

(7) Die Gruppe prüft die Fragen, die der Vorsitzende von sich aus oder auf Antrag eines Vertreters der Kontrollstellen oder auf Antrag der Kommission auf die Tagesordnung gesetzt hat.

10. Anhang

10.3 §§ 11 und 14 Rundfunkbeitragsstaatsvertrag

§ 11 Verwendung personenbezogener Daten

(1) Beauftragt die Landesrundfunkanstalt Dritte mit Tätigkeiten bei der Durchführung des Beitragseinzugs oder der Ermittlung von Beitragsschuldnern, die der Anzeigepflicht nach § 8 Abs. 1 nicht oder nicht vollständig nachgekommen sind, so gelten für die Erhebung, Verarbeitung und Nutzung der dafür erforderlichen Daten die für die Datenverarbeitung im Auftrag anwendbaren Bestimmungen.

(2) Beauftragten die Landesrundfunkanstalten eine Stelle nach § 10 Abs. 7 Satz 1 mit Tätigkeiten bei der Durchführung des Beitragseinzugs und der Ermittlung von Beitragsschuldnern, ist dort unbeschadet der Zuständigkeit des nach Landesrecht für die Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ein behördlicher Datenschutzbeauftragter zu bestellen. Er arbeitet zur Gewährleistung des Datenschutzes mit dem nach Landesrecht für die Landesrundfunkanstalt zuständigen Datenschutzbeauftragten zusammen und unterrichtet diesen über Verstöße gegen Datenschutzvorschriften sowie die dagegen getroffenen Maßnahmen. Im Übrigen gelten die für den behördlichen Datenschutzbeauftragten anwendbaren Bestimmungen des Bundesdatenschutzgesetzes entsprechend.

(3) Die zuständige Landesrundfunkanstalt darf von ihr gespeicherte personenbezogene Daten der Beitragsschuldner an andere Landesrundfunkanstalten auch im Rahmen eines automatisierten Abrufverfahrens übermitteln, soweit dies zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden oder der empfangenden Landesrundfunkanstalt beim Beitragseinzug erforderlich ist. Es ist aufzuzeichnen, an welche Stellen, wann und aus welchem Grund welche personenbezogenen Daten übermittelt worden sind.

(4) Die zuständige Landesrundfunkanstalt kann im Wege des Ersuchens für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach diesem Staatsvertrag besteht, personenbezogene Daten bei öffentlichen und nichtöffentlichen Stellen ohne Kenntnis des Betroffenen erheben, verarbeiten oder nutzen. Voraussetzung dafür ist, dass

1. die Datenbestände dazu geeignet sind, Rückschlüsse auf die Beitragspflicht zuzulassen, insbesondere durch Abgleich mit dem Bestand der bei den Landesrundfunkanstalten gemeldeten Beitragsschuldner, und

2. sich die Daten auf Angaben beschränken, die der Anzeigepflicht nach § 8 unterliegen und kein erkennbarer Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat.

Die Erhebung, Verarbeitung oder Nutzung bei den Meldebehörden beschränkt sich auf die in § 14 Abs. 9 Nr. 1 bis 8 genannten Daten. Daten, die Rückschlüsse auf tatsächliche oder persönliche Verhältnisse liefern könnten, dürfen nicht an die übermittelnde Stelle rückübermittelt werden. Das Verfahren der regelmäßigen Datenübermittlung durch die Meldebehörden nach den Meldegesetzen oder Meldedatenübermittlungsverordnungen der Länder bleibt unberührt. Die Daten Betroffener, für die eine Auskunftssperre gespeichert ist, dürfen nicht übermittelt werden.

(5) Die Landesrundfunkanstalt darf die in Absatz 4 und in § 4 Abs. 7, § 8 Abs. 4 und 5 und § 9 Abs. 1 genannten Daten und sonstige freiwillig übermittelte Daten nur für die Erfüllung der ihr nach diesem Staatsvertrag obliegenden Aufgaben erheben, verarbeiten oder nutzen. Die erhobenen Daten sind unverzüglich zu löschen, wenn feststeht, dass sie nicht mehr benötigt werden oder eine Beitragspflicht dem Grunde nach nicht besteht. Nicht überprüfte Daten sind spätestens nach zwölf Monaten zu löschen. Jeder Beitragsschuldner erhält eine Anmeldebestätigung mit den für die Beitragserhebung erforderlichen Daten.

§ 14 Übergangsbestimmungen

(9) Um einen einmaligen Abgleich zum Zwecke der Bestands- und Ersterfassung zu ermöglichen, übermittelt jede Meldebehörde für einen bundesweit einheitlichen Stichtag automatisiert innerhalb von längstens zwei Jahren ab dem Inkrafttreten dieses Staatsvertrages gegen Kostenerstattung einmalig in standardisierter Form die nachfolgenden Daten aller volljährigen Personen an die jeweils zuständige Landesrundfunkanstalt:

1. Familienname,
2. Vornamen unter Bezeichnung des Rufnamens,
3. frühere Namen,
4. Doktorgrad,
5. Familienstand,
6. Tag der Geburt,
7. gegenwärtig und letzte Anschrift von Haupt- und Nebenwohnungen, einschließlich aller vorhandenen Angaben zur Lage der Wohnung, und
8. Tag des Einzugs in die Wohnung.

Hat die zuständige Landesrundfunkanstalt nach dem Abgleich für eine Wohnung einen Beitragsschuldner festgestellt, hat sie die Daten der übrigen dort wohnenden Personen unverzüglich zu löschen, sobald das Beitragskonto ausgeglichen ist. Im Übrigen darf sie die Daten zur Feststellung eines Beitragsschuldners für eine Wohnung nutzen, für die bislang kein Beitragsschuldner festgestellt wurde; Satz 2 gilt entsprechend. Die Landesrundfunkanstalt darf die Daten

auch zur Aktualisierung oder Ergänzung von bereits vorhandenen Teilnehmerdaten nutzen. § 11 Abs. 5 Satz 2 und 3 gilt entsprechend.

10. Anhang

10.4 §§ 7 bis 9 MDR-Rundfunkbeitragsatzung

§ 7 Datenerhebung bei öffentlichen Stellen

(1) Die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle wird eine andere öffentliche Stelle um die Übermittlung personenbezogener Daten gemäß § 11 Abs. 4 RBStV nur ersuchen soweit eine vorherige Datenerhebung unmittelbar beim Betroffenen erfolglos war oder nicht möglich ist. Dabei werden nur die in § 8 Abs. 4 und 5 RBStV genannten Daten unter den Voraussetzungen von § 11 Abs. 4 Satz 2 RBStV erhoben. Die Verfahren der regelmäßigen Datenübermittlung durch die Meldebehörden nach den entsprechenden Regelungen der Länder und der einmaligen Meldedatenübermittlung nach § 14 Abs. 9 RBStV bleiben unberührt.

(2) Die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle wird personenbezogene Daten nach Absatz 1 bei öffentlichen Stellen nur erheben, um

1. bisher unbekannte Beitragsschuldner festzustellen oder
2. die von ihr gespeicherten Daten von Beitragsschuldnern im Rahmen des Datenkatalogs nach § 8 Abs. 4 und 5 RBStV zu berichtigen, zu ergänzen oder zu löschen.

(3) Die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle wird nur solche öffentlichen Stellen um die Übermittlung personenbezogener Daten ersuchen, die über die Daten einzelner Inhaber von Wohnungen oder einzelner Inhaber von Betriebsstätten verfügen und denen die Übermittlung dieser Daten an die Rundfunkanstalt rechtlich gestattet ist. Diese öffentlichen Stellen sind insbesondere

1. Meldebehörden,
2. Handelsregister,
3. Gewerberegister und
4. Grundbuchämter.

(4) Auf das datenschutzrechtliche Auskunftersuchen eines Beitragsschuldners wird die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle dem Beitragsschuldner die öffentliche Stelle mitteilen, die ihr die jeweiligen Daten des Beitragsschuldners übermittelt hat.

§ 8 Datenerhebung bei nicht-öffentlichen Stellen

(1) Die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle darf ein Auskunftsverlangen an die in § 9 Abs. 1 Satz 2 und 3 RBStV genannten Personen nur richten, wenn ein vorheriges Auskunftsverlangen beim Betroffenen nach § 9 Abs. 1 Satz 1 RBStV und eine Anfrage bei der Meldebehörde oder dem maßgeblichen öffentlichen Register nach § 7 Abs. 3 erfolglos geblieben ist oder nicht möglich war. Die Auskunft ist schriftlich zu erteilen und auf die Daten nach § 8 Abs. 4 Nr. 3 RBStV der jeweiligen Inhaber der betreffenden Wohnung oder Betriebsstätte beschränkt.

(2) Vorbehaltlich der Regelungen in Absatz 1 darf die Rundfunkanstalt oder die in § 2 genannte gemeinsame Stelle als nicht-öffentliche Stelle nur Unternehmen des Adresshandels und der Adressverifizierung um die Übermittlung personenbezogener Daten gemäß § 11 Abs. 4 RBStV im Rahmen der dort in Satz 2 genannten Beschränkungen ersuchen. § 14 Abs. 10 RBStV ist zu beachten. § 7 Abs. 2 Nr. 1, Abs. 3 Satz 1 und Abs. 4 gelten entsprechend.

§ 9 Technisch-organisatorischer Datenschutz

Es ist sicherzustellen, dass bei der in § 2 genannten gemeinsamen Stelle ein wirksames und übergreifendes Informationssicherheits-Managementsystem instal-

liert und die Löschung der Daten von Rundfunkteilnehmern und Beitragsschuldern nach einem einheitlichen Konzept geregelt wird.

10. Anhang

10.5 Verfahrenskodex der Rundfunkbeauftragten für den Datenschutz

Behandlung von datenschutzrechtlichen Anfragen, Beschwerden und Auskunftsverlangen

(1) Die Rundfunkbeauftragten für den Datenschutz [RfD] sind bestrebt, Eingaben oder Hinweise Dritter möglichst zeitnah und effizient zu bearbeiten. Damit soll zum einen eventuellen Missständen abgeholfen werden, aber es sollen auch im jeweiligen Verantwortungsbereich der RfD geeignete Maßnahmen getroffen werden können, die datenschutzrechtliche Standards ergänzen und verbessern.

(2) Die RfD unterstützen den Bürger bei der konkreten Wahrung seines individuellen Rechts auf informationelle Selbstbestimmung im Bereich des Rundfunkwesens; dementsprechend werden Auskünfte zu allgemeinen datenschutzrechtlichen Fragen nachrangig und – soweit möglich – formalisiert erteilt.

(3) Die RfD nehmen Eingaben oder Hinweise vorzugsweise in schriftlicher Form (Brief, Telefax, E-Mail, evtl. SMS) entgegen. Dadurch werden Missverständnisse vermieden und die Legitimation des Petenten leichter nachvollziehbar gemacht. Werden Eingaben oder Hinweise einem RfD mündlich vorgetragen, wird er aus den dargelegten Gründen regelmäßig darum bitten, schriftlich über das konkrete Anliegen informiert zu werden.

(4) In Fällen besonderer Dringlichkeit oder der Verhinderung des Petenten an einem schriftlichen Vortrag oder bei unkomplizierten, kurzfristig zu klärenden Sachverhalten erledigt der RfD den Vorgang ggf. auch aufgrund (fern-) mündlicher Anfrage.

(5) Bei der Entgegennahme von Eingaben oder Hinweisen prüft der RfD, u. a. um seine eigene territoriale Zuständigkeit sicherzustellen, die Identität des Petenten; dabei ist mindestens der genaue Name und die Wohnanschrift festzustellen; bei Eingaben, die das Rundfunkgebührenwesen betreffen, verschafft sich der RfD ggf. auch Kenntnis über die Teilnehmernummer. Bei Zweifeln an der Geschäftsfähigkeit - so u. a. evtl. an der Volljährigkeit - eines Petenten stellt der RfD erforderliche Informationen sicher. Soweit der Petent nicht bereit ist, sich zu identifizieren oder erkennbar ungenaue Angaben macht, ist der RfD nicht verpflichtet, sich auf andere Weise Gewissheit über die Identität des Petenten zu verschaffen. Bei fehlenden Anhaltspunkten oder Zweifeln an der Identität eines Petenten ist der RfD berechtigt, eine Behandlung oder Bearbeitung der Eingabe oder des gegebenen Hinweises zu verweigern.

(6) Eine Eingabe oder ein Hinweis hat mindestens so bestimmt zu sein, dass der aufgegriffene Sachverhalt und das konkrete Anliegen verständlich sind. Mangelt es im Einzelfall lediglich an bestimmten Detailangaben, stellt der RfD durch gezielte Nachfrage beim Petenten die vollständige Aufklärung des Sachverhaltes oder Anliegens sicher. Ist weder eine Sachverhalts- noch eine Anliegensklärung möglich, beendet der RfD die Behandlung der Angelegenheit. Der RfD behandelt regelmäßig keine Eingaben oder Hinweise beleidigenden Inhalts oder in herabwürdigender Form vorgetragene Anliegen.

(7) Der RfD wickelt seine Korrespondenz aus Gründen der Vertraulichkeit und Datensicherheit grundsätzlich nur auf dem Briefweg ab. Andere Kommunikationswege (Telefax, E-Mail oder SMS) werden durch den RfD nur verwendet, wenn sie zuvor mit dem Petenten abgestimmt wurden oder der Petent sich seinerseits durch Form und Darstellung in seiner Eingabe mit einer Abwicklung auf einem anderen Kommunikationsweg einverstanden gezeigt hat.

(8) Ist der RfD aufgrund der für ihn erkennbaren Umstände nach eigener Einschätzung nicht in der Lage, zu einer Eingabe oder einem Hinweis kurzfristig (i. e. regelmäßig binnen eines Monats nach Erhalt) abschließend Stellung zu nehmen, erteilt er dem Petenten einen Zwischenbescheid.

(9) Wird die Angelegenheit von dritter Seite an den RfD abgegeben, bestätigt der RfD dem Übermittelnden die Übernahme der Angelegenheit dann, wenn dies nicht bereits durch die abgebende Stelle geschehen ist oder die abschließende Beantwortung der Eingabe nicht zeitnah erfolgen kann.

(10) Bei sich langfristig hinziehenden Angelegenheiten lässt der RfD einem Petenten in regelmäßigen Abständen - ca. alle drei Monate – unaufgefordert eine Zwischennachricht zukommen. RfD stellt bei Vornahme seiner Recherchen und den ggf. anschließend von ihm ergriffenen oder eingeleiteten Maßnahmen die nötige Vertraulichkeit sicher, die verhindert, dass dem Petenten wegen seiner Kontaktaufnahme mit dem RfD irgendwelche Nachteile erwachsen.

(11) Der RfD erteilt dem Petenten nach Abschluss der Bearbeitung eine Nachricht, in der in angemessener Form und gebotenem Umfang über die getroffenen Feststellungen und ergriffenen Maßnahmen berichtet wird. Der RfD erhebt für seine Tätigkeit keine Gebühren oder Entgelte vom Petenten. Rückfragen des Petenten zu der ihm abschließend erteilten Nachricht behandelt der RfD, soweit dem Anliegen des Petenten damit noch zusätzlich Rechnung getragen werden kann.

(12) Der RfD berichtet über Angelegenheiten von besonderer Bedeutung oder außerordentlicher Tragweite in anonymisierter Form in seinem Tätigkeitsbericht.

10. Anhang

10.6 Mitglieder des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB)

Rundfunkanstalt	Datenschutzbeauftragte/r
ARTE Deutschland TV GmbH	Christoph Weber
Bayerischer Rundfunk	Barbara Nickel Referat: Monika Moser
Deutsche Welle	Thomas Gardemann
Deutschlandradio	Dr. Markus Höppener Referat: Ulla Pageler
Beitragsservice	Kerstin Arens Referat: Christian Kruse
Hessischer Rundfunk	Ulrich Göhler
Mitteldeutscher Rundfunk	Stephan Schwarze
Norddeutscher Rundfunk	Horst Brendel Stellvertreterin: Cornelia Weitzel-Kerber
Radio Bremen	Sven Carlson
Rundfunk Berlin Brandenburg	Anke Naujock Stv. behördlicher DSB: Dr. Hans Bismark
Saarländischer Rundfunk	Sonia Wüst
Südwestrundfunk	Prof. Dr. Armin Herb Referat: Marianne Gottheil
Westdeutscher Rundfunk	Beate Ritter Referat: Günter Griebach
Zweites Deutsches Fernsehen	Christoph Bach
Kinderkanal ARD/ZDF	Jörn Voss