MITTELDEUTSCHER RUNDFUNK
Anstalt des öffentlichen Rechts

DATENSCHUTZBEAUFTRAGTER

Tätigkeitsbericht des Beauftragten für den Datenschutz des MDR für den Zeitraum 01.07.2014 bis 30.06.2016

Stephan Schwarze

Inhaltsverzeichnis

10. Anhang

1. Einleitung

Der Verwaltungsrat hat mich erstmalig in seiner Sitzung am 18.06.2012 auf Vorschlag der Intendantin gem. § 42 MDR-Staatsvertrag als Beauftragten für den Datenschutz des MDR für die Dauer von vier Jahren bestellt. Am 13.06.2016 hat mich der Verwaltungsrat des MDR für weitere vier Jahre zum Datenschutzbeauftragten des MDR berufen. Mit diesem Bericht komme ich meiner Pflicht aus § 42 Abs. 8 des MDR Staatsvertrages nach, wonach der Datenschutzbeauftragte den Organen der Rundfunkanstalt einen Bericht über seine Tätigkeit vorlegen muss. Der Bericht ist der dritte meiner zurückliegenden Amtszeit und behandelt meine Tätigkeit im Zeitraum 01.07.2014 bis 30.06.2016. Damit kehre ich zurück in den zweijährigen, vom Staatsvertrag vorgesehenen, Rhythmus.

Im Berichtszeitraum mussten keine förmlichen Beanstandungen ausgesprochen werden. Die frühzeitige Einbindung des Datenschutzbeauftragten in die Prozesse erleichtert meine Arbeit ungemein.

Besonders bedanken darf ich mich wiederum bei der Abteilung IT-Sicherheit des MDR. Datenschutz ist ohne die Sicherheit der IT-Systeme nicht realisierbar. Bei allen technischen Fragen standen mir Elisabeth Kunath und ihr Team jederzeit mit Rat und Tat zur Seite, was ich sehr zu schätzen weiß. Ebenso bedanke ich mich bei meinem Abwesenheitsvertreter Dr. Bernd Appel, der viele wertvolle Impulse zum Datenschutz beim MDR gegeben hat.

Gemeinsam mit dem Datenschutzbeauftragten des ZDF, Herrn Christoph Bach, bin ich zuständig für den Datenschutz beim Kinderkanal von ARD und ZDF (KiKA). Hier gebührt mein Dank neben Herrn Bach besonders Herrn Jörn Voss, der als betrieblicher Datenschutzbeauftragter des KiKA dort die Fäden fest in der Hand hält und vor Ort für reibungslose Abläufe sorgt. Dass auf Kinderdaten besonders geachtet werden muss, versteht sich von selbst. Der Schutz dieser Daten soll aber nicht dazu führen, dass Kindern der Zugang zu der Medien- und Onlinewelt versperrt bleibt. Datenschutz auf Kosten der Medienkompetenz kann

nicht das Ziel sein, vielmehr müssen diese beiden Hand in Hand gehen. Dies ist Aufgabe und Ansporn gleichermaßen.

Ich ziehe ein positives Resümee der zweiten Hälfte meiner Amtszeit. Unterschiedliche Themen, die in diesem Bericht auszugsweise angesprochen werden und eine bemerkenswerte Aufgeschlossenheit für die Belange des Datenschutzes haben diese Zeit geprägt. Der intensive Austausch mit den Kolleginnen und Kollegen von ARD und ZDF erwies sich als ertragreich und lohnend. Hier wird besonders auf den sorgsamen Umgang mit den Beitragszahlerdaten geachtet.

Die Arbeit erwies sich als spannend und befriedigend. Der Kontakt mit unterschiedlichen Kollegen und die Auseinandersetzung mit stets neuen Themen erfordern Aufmerksamkeit, machen aber auch sehr viel Spaß. Ich hoffe, dass ich noch weiter in diese Aufgabe hineinwachsen kann und freue mich auf die nächsten vier Jahre als Beauftragter für den Datenschutz des Mitteldeutschen Rundfunks.

2. Aufgaben des Datenschutzbeauftragten

Die Rechtsgrundlagen für den Datenschutzbeauftragen 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 Anstalten 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 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.

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

Am 14.04.2016 wurde die Datenschutz-Grundverordnung (DS-GVO) vom EU-Parlament beschlossen Sie ersetzt die aus dem Jahr 1995 stammende Richtlinie 95/46/EG (Datenschutzrichtlinie). In meinen letzten Berichten hatte ich die Entwicklung und die Schwierigkeiten bei der Verabschiedung dieser Grundverordnung bereits geschildert.

Bemerkenswert ist zunächst, dass dieses Regelwerk unmittelbar gilt und nicht nur den nationalen Gesetzgeber zur Anpassung verpflichtet, wie dies etwa eine Richtlinie täte. Zwar ist diese Grundverordnung jetzt beschlossen worden, Geltung haben wird sie aber erst ab dem 25.05.2018, sodass bis dahin die derzeitige Rechtslage fortbesteht. Obwohl die Grundverordnung unmittelbar geltendes Recht ist, ist auf europäischer aber auch auf nationaler Ebene Raum für ergänzende Regelungen. Es gibt ca. 50 bis 60 sogenannte Öffnungsklauseln, die mit weiteren Regelungen befüllt werden können. Dieser Handlungsspielraum ist jedoch insoweit begrenzt, da das mit der Verordnung gewollte Prinzip der Vollharmonisierung als unabdingbare Vorgabe gilt. Daher sollte eher von ergänzenden Regelungsbefugnissen gesprochen werden.

Die DS-GVO schreibt im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien fort und entwickelt sie weiter. Die aus der EU-Datenschutzrichtlinie und den deutschen Datenschutzgesetzen bekannten Grundsätze des „Verbots mit Erlaubnisvorbehalt“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“ und der „Transparenz“ prägen auch die DS-GVO. Die Verordnung enthält jedoch auch einige neue Elemente. Zum einen ist in diesem Zusammenhang das sog. Marktortprinzip zu nennen, nach dessen Maßgabe das EU-Datenschutzrecht auch für Wirtschaftsunternehmen außerhalb der Europäischen Union gilt. Voraussetzung ist lediglich, dass sich ein Angebot an einen bestimmten nationalen Markt in der EU richtet oder dass die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU

dient. Interessant wird in diesem Zusammenhang unter anderem die Entwicklung bei den sog. sozialen Netzwerke wie z. B. bei Facebook oder Twitter werden. Diese Anbieter erfüllen derzeit aus verschiedenen Gründen nicht die deutschen Datenschutzstandards. Bedenken bestehen insbesondere im Hinblick auf die Anforderungen an Transparenz, Datensparsamkeit und wirksame Einwilligung. Die meisten Anbieter speichern die Daten zudem außerhalb der EU in Ländern wie den USA, die kein vergleichbares Niveau an Datenschutz gewährleisten. Es bleibt abzuwarten, ob diese Unternehmen vor dem Hintergrund der DS-GVO hier nachbessern.

Eine für den öffentlich-rechtlichen Rundfunk bedeutsame Öffnungsklausel findet sich in Artikel 85 der DS-GVO. Dort wird die Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit geregelt. Nach Abs. 1 müssen die Mitgliedsstaaten durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung, einschließlich der Verarbeitung zu journalistischen Zwecken, in Einklang bringen. Damit ist den Landesgesetzgebern die Aufgabe zugewiesen, entsprechende Datenschutzregelungen zu schaffen, die den Auftrag einer Rundfunkanstalt wie dem MDR berücksichtigen und journalistische Aufgaben und die Belange des Datenschutzes verbinden. Sie müssen sich auch mit der Frage beschäftigen, wie die Datenschutzaufsichtsbehörden auszugestalten sind, sich also mit den Aufgaben der Rundfunkdatenschützer befassen.

Auf Ebene des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio wird gerade das letztgenannte Thema besonders aufmerksam beobachtet. Auch müssen die vielfältigen Fragen geklärt werden, wie sich die einzelnen Vorgaben der Grundverordnung auf die Datenschutzrealität in den Rundfunkanstalten auswirkt. Eine Unterarbeitsgruppe des Arbeitskreises der Datenschutzbeauftragten befasst sich damit und wird im Laufe des Jahres 2016 zu Ergebnissen kommen. Insgesamt ist es aber von großer Wichtigkeit, dass die Unabhängigkeit des Rundfunkdatenschutzes erhalten bleibt, damit eine staatliche Einflussnahme auf diesem Wege ausgeschlossen ist.

Obwohl die Grundverordnung mittlerweile beschlossen ist, sind noch viele Frage offen und die Umsetzung zu klären. Es bleibt also spannend und erfordert große Aufmerksamkeit.

3. Entwicklung des Datenschutzrechts

3.2 Auswirkungen der Safe Harbor-Entscheidung

Zwischen der Europäischen Union und den Vereinigten Staaten von Amerika war im Jahre 2000 eine Vereinbarung getroffen worden, die gewährleisten sollte, dass personenbezogene Daten legal in die USA übermittelt werden können. Hintergrund war, dass in den USA kein dem Niveau der EU vergleichbarer Datenschutzstandard vorhanden ist. In den USA tätige Unternehmen konnten gem. der Vereinbarung dem Safe Harbor-Abkommen beitreten, in dem Sie sich verpflichteten, bestimmte Prinzipien einzuhalten. Im Wesentlichen handelte es sich dabei um eine Informationspflicht, nach der die Unternehmen die Betroffenen darüber unterrichten mussten, welche Daten sie für welche Zwecke verarbeiten. Ebenso musste über die Weitergabe der Daten informiert und die für ein angemessenes Sicherheitsniveau gesorgt werden. Zudem war die Datenintegrität zu gewährleisten, die Unternehmen hatten also sicherzustellen, dass die von ihnen erhobenen Daten korrekt, vollständig und zweckdienlich sind. Mit Urteil vom 06.10.2015 hat der EuGH Safe Harbor für ungültig erklärt. Im Wesentlichen hat der EuGH deswegen so entschieden, weil die Vereinbarung über Safe Harbor mit den USA einen Zugriff staatlicher Behörden nicht ausschließen könne. Außerdem seien gegen Eingriffe in die Rechte von EU-Bürgern keine Rechtsbehelfe gegeben.

Im Februar 2016 ist eine neue Vereinbarung mit den USA, genannt „Privacy-Shield“, geschlossen worden. Die US-Administration hat der EU-Kommission einen besseren Schutz für Daten aus der EU schriftlich zugesichert. Unter anderem sollen Überwachungsmaßnahmen auf das „Notwendige und Verhältnismäßige“ begrenzt werden und jährliche Berichte von US-Seite an die Kommission ergehen. Ungeachtet der Kritik der Europäischen Datenschutzbehörden und des Eu-

ropäischen Parlaments am Privacy Shield, dass auch dieses Abkommen massenhaft Informationen im Dienste der öffentlichen Sicherheit zu sammeln ermögliche, haben die meisten EU-Staaten den neuen - nachgebesserten - Regeln für den Datenaustausch zugestimmt. Daraufhin hat die EU-Kommission das Privacy Shield am 12. Juli 2016 förmlich verabschiedet. Sie wird jährlich einen Bericht über die Erfahrungen mit dem Privacy Shield erstellen und diesen dem Europäischen Parlament und dem Europäischen Rat zuleiten. Die Überprüfung wird von der Kommission gemeinsam mit dem US-Handelsministerium durchgeführt. Es wird allerdings schon jetzt bezweifelt, dass Privacy Shield den Anforderungen des EuGH genügen würden, falls eine Klage dagegen erhoben würde.

Für den MDR spielt das ganze Thema insofern eine Rolle, dass die Server für Streamingdienste teilweise in den USA stehen. Wenn nun die IP-Adressen der deutschen und europäischen Nutzer in die USA transferiert werden, besteht ein Problem. Bei der Neuausschreibung der Streamingdienste im Juni 2016 wurde daher die Forderung aufgestellt, dass die Server in der EU stehen und keine Daten in die USA übertragen werden dürfen. Zum Zeitpunkt dieses Berichtes war noch keine abschließende Entscheidung getroffen worden.

Auch die Nutzung von Cloud-Diensten, also die Nutzung von Rechen- und Speicherkapazitäten über das Internet, wirft in diesem Zusammenhang Probleme auf. Es werden Infrastrukturen angemietet, die Speicherlösungen anbieten, aber auch zugeschnittene Softwarelösungen bereitstellen können. Dabei werden auch personenbezogenen Daten verarbeitet, möglicherweise in den USA. Daher ist es sehr wichtig, dass das Thema des Datenaustausches mit den USA auf eine stabile rechtliche Grundlage gestellt wird.

Unabhängig davon wird die Frage diskutiert, ob mit sog. EU-Standardvertragsklauseln beim transatlantischen Datenverkehr gearbeitet werden kann. Die EU hat zu dem Zweck, ein angemessenes Datenschutzniveau auch mit den USA zu gewährleisten, diese Vertragsklauseln entwickelt. Hier werden die Vertragspartner verpflichtet, für ein angemessenes Datenschutzniveau zu sorgen. Allerdings ist auch dieser Weg zurzeit mit Unsicherheiten behaftet, da

nicht klar ist, ob diese Klauseln den EuGH-Anforderungen genügen. Gleichwohl bieten die Standardvertragsklauseln weiterhin eine vernünftige Möglichkeit, einen legalen Datentransfer in die USA sicherzustellen. Dennoch ist es auch Sicht der Datenschutzbeauftragten von ARD und ZDF vorzugswürdig, keine Daten in die USA zu transferieren, zumindest dafür zu sorgen, dass nur anonymisierte und damit nicht mehr personenbezogene Daten an die USA übermittelt werden.

3. Entwicklung des Datenschutzrechts

3.3 Bundesrecht

3.3.1 Informationssicherheitsgesetz

Am 25. Juli 2015 ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (Informationssicherheitsgesetz) als Artikelgesetz in Kraft getreten. Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen müssen künftig einen Mindeststandard an Informationssicherheit einhalten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Darüber hinaus sind zur Steigerung der Informationssicherheit die Anforderungen an die Anbieter von Telekommunikations- und Telemediendiensten erhöht worden. Parallel dazu sind die Kompetenzen des BSI und der Bundesnetzagentur sowie die Ermittlungszuständigkeiten des Bundeskriminalamtes (BKA) im Bereich der Computerdelikte ausgebaut worden. Den Kritikern geht das Gesetz nicht weit genug. Es wird moniert, dass es in dem Gesetz zu viele unbestimmte Rechtsbegriffe gibt. Die vorgesehenen Maßnahmen seien nicht geeignet, zur Erhöhung der Informationssicherheit in Deutschland beizutragen. Vor dem Hintergrund der sensiblen Informationen, die das BSI durch die Meldungen von Sicherheitsvorfällen erhalte, wird zudem eine unabhängige Stellung des BSI, das derzeit dem Bundesinnenministerium unterstellt und verpflichtet ist, gefordert. Die Landesrundfunkanstalten gehören zum Sektor der kritischen Infrastrukturen Medien und Kultur. Dieser Sektor untersteht aber der Gesetzgebung der Länder. Aus diesem Grund sind die Landesrundfunkanstalten nicht Ad-

ressaten dieses Bundesgesetzes. Dass zumindest Medien durchaus als kritische Infrastrukturen gefährdet sind, dürfte jedoch nach dem groß angelegten Angriff auf die französische Fernsehsendergruppe TV5Monde Anfang April 2015 inzwischen einhellige Meinung sein. Insoweit empfiehlt es sich, dass sich der MDR an dem im Informationssicherheitsgesetz vorgeschriebenen Mindeststandard an Informationssicherheit zumindest orientiert. Auch vor diesem Hintergrund halte ich es für notwendig, die Themen Datenschutz und Informationssicherheit im MDR weiter durch Bereitstellung von Ressourcen zu stärken. Im Übrigen sind die legislativen Entwicklungen auf diesem Gebiet weiterhin sehr aufmerksam zu verfolgen.

3.3.2 Telemediengesetz

Am 27. Juli 2016 ist das geänderte Telemediengesetz (TMG) in Kraft getreten. Mit der Gesetzesänderung soll klargestellt werden, dass Betreiber von öffentlichen Funknetzen (WLAN) ebenso von der Haftung für Rechtsverstöße Dritter freigestellt sind wie Festnetzanbieter.
Von dieser Gesetzesänderung ist der MDR unmittelbar betroffen. Denn auch er bietet seinen Gästen und Mitarbeitern mittlerweile WLAN an.
Der Gesetzesänderung ging ein jahrelanges Tauziehen voraus, an dessen Ende ein Kompromiss steht, der von Experten kritisiert wird. Erst die Praxis wird zeigen, ob die Gesetzesänderung tatsächlich auch vor zivilrechtlicher Inanspruchnahme des WLAN-Betreibers schützt.
Möglicherweise wird es im Laufe des Jahres noch eine neue Entwicklung geben. Denn in einem beim EuGH anhängigen Verfahren, das das Münchner Landgericht vorgelegt hatte, wird dieser Ansprüche von Sony Music gegen eine Person, die ein offenes WLAN betreibt, prüfen.

4. Datenschutz im MDR

4.1 Kundenbeziehungsmanagement

Der MDR steht vor der Aufgabe, eine bereichsübergreifende Publikumskommunikation zu etablieren, die alle Dialogwege umfasst. Hintergrund sind die Erwartungen der Kunden/Beitragszahler an ein serviceorientiertes Beschwerdemanagement sowie verbesserte Kommunikation über die Angebote des MDR. Außerdem soll die individuelle Information über Angebote und potenzielle Interessen verbessert werden.

Dieser Ansatz wirft Datenschutzfragen auf. Es verbietet sich natürlich, einfach die Daten von Zuschauern und Zuhörern zu sammeln und für Zwecke der Kundenkommunikation wahllos einzusetzen. Der MDR muss sich an das Sächsische Datenschutzgesetz halten und kann Daten zunächst nur dann verarbeiten, wenn dies für seinen Auftrag notwendig ist. Als Lösung bleibt also lediglich, den Kontakt mit den Kunden zu nutzen, um ihre Einwilligung in eine vorher festgelegte Kommunikation einzuholen. Es ist also erforderlich, einen relativ hohen Aufwand zu betreiben und die Kunden dahingehend zu befragen, ob sie in einem bestimmten Rahmen über weitere Angebote informiert werden wollen. Hier muss der Zweck möglichst genau umrissen werden und auch der Kunde darüber aufgeklärt werden, was mit seinen Daten geschieht. Letztendlich treffen den MDR in diesem Zusammenhang auch Auskunftspflichten, es muss also immer klar sein, wo die Daten vorgehalten und wie lange sie aufbewahrt werden. Hierzu habe ich eine Schulung angeboten und war im Berichtszeitraum mit der zuständigen Arbeitsgruppe in engem Austausch. Der Datenschutz darf hier auf keinen Fall vernachlässigt werden, denn ein transparenter und sicherer Umgang mit Kundendaten schafft das notwendige Vertrauen, um eine stabile Kundenbeziehung zu gewährleisten.

4. Datenschutz im MDR

4.2 Datenträgerentsorgung

Ein Thema, mit dem sich Datenschutzbeauftragte seit jeher beschäftigen müssen, ist die sachgerechte Entsorgung von Daten. Die Verarbeitung von Daten endet in gesetzmäßiger Weise mit ihrer Löschung, sobald sie nicht mehr benötigt werden oder ihre Speicherung unzulässig ist. Oftmals fällt einfach „Datenmüll" an, also Daten, die gar nicht aufbewahrt werden sollen. Dies ist insbesondere in Büros der Fall, wo manchmal achtlos mit papiergebundenen Daten umgegangen wird. In diesem Zusammenhang darf nicht vergessen werden, dass auf jedem Fehldruck eines Briefes oder einer nicht mehr benötigten Kopie auch personenbezogene Daten in den normalen Müll gelangen. Oftmals wird übersehen, dass hier auch Adressen, Telefonnummern oder sonstige personenbezogene Inhaltsdaten vorzufinden sind, die so entsorgt werden sollten, dass die Daten nicht mehr wiederherstellbar sind. Natürlich ist es in vielen Fällen unkritisch, aber dennoch muss sorgsam mit diesen Daten umgegangen werden.

Beim MDR wird angestrebt, die Entsorgung von Datenträgern neu auszuschreiben, dies habe ich gemeinsam mit der Abteilung IT-Sicherheit des MDR zum Anlass genommen, Empfehlungen zur Datenträgerentsorgung zu erarbeiten. Hier wird unterschieden zwischen der Entsorgung von Papier und sonstigen Speichermedien, wie beispielsweise CDs und DVDs, Festplatten aber auch Speichersticks. Diese Empfehlungen basieren auf einer DIN zur Vernichtung von Datenträgern, in der bestimmte Sicherheitsstufen der Vernichtung hinsichtlich der Vertraulichkeit von Informationen vorgesehen werden. Hier konnte dem verantwortlichen Gebäudemanagement insofern geholfen werden, dass für die Ausschreibung eines entsprechenden Entsorgungsvertrages mit einer Fremdfirma Kriterien und Anforderungen beschrieben werden, die eingehalten werden müssen. In diesem Zusammenhang darf nicht vergessen werden, dass der MDR für die datenschutzgerechte Entsorgung vollständig verantwortlich bleibt, auch wenn er ein Unternehmen damit beauftragt. Es bedarf also einer sorgfältigen Auswahl des Vertragspartners und des Abschlusses eines sogenannten Auftragsdatenverarbeitungsvertrages, der den gesetzlichen Anforderungen genügt. Die

beste Entsorgung nutzt natürlich auch nur dann etwas, wenn die Mitarbeiterinnen und Mitarbeiter des MDR sensibilisiert werden und sich an die Vorgaben halten. Um diesen Zweck zu erreichen, sind Schulungen vorzusehen, die die Aufmerksamkeit auf dieses Thema lenken.

4. Datenschutz im MDR

4.3 IST-Personalanalyse

Im Rahmen von Umstrukturierungen innerhalb des MDR bestand die Anforderung, mit Personaldaten umzugehen: Will man Strukturen verändern, muss man auch schauen, wie das Personal neu aufgeteilt werden kann. Dafür ist es zweifellos notwendig, eine IST-Analyse des Personalbestandes vorzunehmen und sich ggf. zu überlegen, wie die Mitarbeiterinnen und Mitarbeiter in Zukunft eingesetzt werden sollen. Folglich kam man bereits am Anfang der Projektarbeit auf mich zu mit der Frage, wie die Personaldimensionierung und die damit vorgesehene Datenerhebung und -verarbeitung in datenschutzgerechter Weise vorgenommen werden kann.

Die datenschutzrechtliche Bewertung bemisst sich immer an der zentralen Frage des Zweckes der jeweiligen Datenverarbeitung. Dieser Zweck muss den gesetzlichen Vorgaben genügen. Wenn es um Personaldaten geht, muss beim MDR § 37 des Sächsischen Datenschutzgesetzes herangezogen werden. Hier ist unter anderem festgelegt, dass eine Verarbeitung von Personaldaten zur Durchführung organisatorischer und personeller Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes rechtmäßig ist, wenn sie unumgänglich ist. Im vorliegenden Fall konnte daher relativ leicht entschieden werden, dass die Nutzung von Daten für eine Umstrukturierung selbstverständlich in Ordnung ist. Es muss aber auf die Feinheiten geachtet werden: Es ist sicherzustellen, dass nur ein Minimum an tatsächlich erforderlichen Daten verarbeitet wird und dass nur diejenigen, die auch für das Projekt Verantwortung tragen, auf diese Daten zugreifen können. Dies bedeutet demzufolge nicht, dass diese Daten frei verfügbar sind und damit nicht vertraulich zu behandeln sind. Die An-

forderungen an die Datensicherheit bestehen nach wie vor. Insoweit konnte ich mit diesen Hinweisen grünes Licht für die IST-Personalanalyse im Rahmen des Umstrukturierungsprozesses geben.

4. Datenschutz im MDR

4.4 SAP-gestützte Personalkostenplanung

Die Personalkostenplanung findet naturgemäß in der Hauptabteilung Personal und Organisationsentwicklung statt. Dies soll zukünftig ausschließlich SAP-gestützt durchgeführt werden. Damit stand im Raum, für das entsprechende Modul „HCM“ Berechtigungen für Mitarbeiterinnen und Mitarbeiter des MDR zu erteilen, die nicht in der HA Personal und Organisationsentwicklung tätig sind, um Controlling-Aufgaben zu erledigen. Hier wurde an mich die Frage herangetragen, ob dies aus datenschutzrechtlicher Sicht zulässig sein kann, da möglicherweise die Verarbeitung von Personaldaten der Personalabteilung vorbehalten sei.

Nach intensivem Austausch von Argumenten sowohl der einen als auch der anderen Seite bin ich zu dem Ergebnis gekommen, dass dies nicht per se unzulässig ist. Richtig ist, dass die Verarbeitung von Personaldaten des MDR strengen gesetzlichen Anforderungen unterfällt. So muss man sich die Notwendigkeit von Datenverarbeitungsschritten vergegenwärtigen. Außerdem sollte mit Personaldaten sparsam umgegangen werden, so dass es nicht zu einem „Wildwuchs“ kommt. Dennoch war diese Frage letztendlich aus datenschutzrechtlicher Sicht nicht zu entscheiden. Der MDR muss sich darüber im Klaren sein, welche Aufgaben er an welcher Stelle ansiedeln möchte. Wenn bei der Personalkostenplanung auch um Controlling-Aufgaben anfallen, so kann es durchaus notwendig im Sinne des Datenschutzes sein, Personaldaten für diesen Zweck auch außerhalb der Personalabteilung zu verarbeiten. Wenn die Zweckbindung und die Verarbeitungsschritte für die Daten geklärt sind, kann nicht der Standpunkt vertreten werden, dass grundsätzlich Personaldaten ausschließlich in der Personalabteilung verarbeitet werden dürfen.

Sehr positiv habe ich vermerkt, dass die Frage des Datenschutzes an dieser Stelle sehr ernst genommen wird. Dennoch musste ich darauf hinweisen, dass zunächst im MDR zwischen den Bereichen geklärt sein muss, wie eine Personalkostenplanung gemeinsam realisiert werden soll. Dabei sind natürlich Datenschutzvorgaben zu beachten. Im Ergebnis ist dies ein aus meiner Sicht gutes Beispiel für eine gelungene Zusammenarbeit.

4. Datenschutz im MDR

4.5 Qualitätscontrolling-Tool Q-Cep

Das Zentrale Produktionsmanagement des MDR hat ein Qualitätscontrolling-Tool entwickelt, das die objektive Beurteilung der Eignung und Fähigkeit der verschiedenen Vertragspartner des MDR wiedergeben und ein einheitliches, transparentes Mängelmanagement ermöglichen soll. Damit wird eine Grundlage geschaffen für die Auswahl geeigneter Dienstleister, je nach der programmlichen Aufgabenstellung.

In diesem System wird nur die Bezeichnung der Dienstleister verarbeitet, und es ist erkennbar, wer die Dienstleister bewertet hat. Zweck der Maßnahme ist die Beurteilung von Leistungen der Geschäftspartner und ein damit verbundenes Qualitätsmanagement. Organisatorisch ist sichergestellt, dass keine Leistungs- und Verhaltenskontrolle der bewertenden Mitarbeiter des MDR möglich ist. Ich habe darauf gedrungen, dass keine personenbezogenen Daten der Dienstleister in dem System erfasst werden, so dass es tatsächlich nur um die objektive Leistungsfähigkeit der beauftragten Unternehmen geht und nicht zugleich „schwarze Listen“ von Mitarbeitern dieser Fremdfirmen geführt werden. Ebenso habe ich darauf hingewiesen, dass der Zugriff auf diese Datenbank reglementiert werden muss, so dass nur diejenigen davon Kenntnis erhalten, die tatsächlich damit arbeiten, also Aufträge auslösen müssen. Im Zuge dessen habe ich meine datenschutzrechtliche Zustimmung erteilt.

Der Personalrat wies mich in diesem Zusammenhang auf ein zusätzliches Problem hin. Zwar ist sichergestellt, dass die Datenerfassung nur die Leistung von Firmen und nicht der einzelnen Mitarbeiter umfasst, jedoch besteht die theoretische Gefahr, dass die erfassten Daten bestimmten Personen zugeordnet werden können, wenn entsprechendes Zusatzwissen besteht.

Damit ist nicht auszuschließen, dass sich nachträglich zuordnen lässt, welcher Beschäftigte des Dienstleisters (ggf. Tochterunternehmen des MDR) die kritisierte Leistung erbracht hat. Ich habe in diesem Zusammenhang auf die sogenannte Zweckbindung verwiesen. Es muss bei personenbezogenen Daten stets klar sein, zu welchem Zweck sie genutzt werden sollen. In dem konkreten Fall sollten überhaupt keine personenbezogenen Daten erhoben werden, so dass es keinen legitimen Zweck gibt, mit personalisierten Daten in diesem Zusammenhang zu arbeiten. Selbstverständlich ist es möglich, dass aufgrund persönlicher Erfahrungen bekannt ist, welche Person sich hinter einer konkreten Dienstleistung verbirgt. Dieses Zusatzwissen darf jedoch keinesfalls für einen irgendwie gearteten Zweck verwendet werden. Natürlich lässt sich so ein Zusatzwissen kaum verhindern. Es muss jedoch organisatorisch dafür gesorgt werden, dass dieses Wissen nicht verwendet wird. Auf diesen Umstand ist bei der Anwendung und Schulung der Software eindringlich hinzuweisen. Eine Bildung von persönlichen Profilen ist in jedem Fall auszuschließen.

Aus datenschutzrechtlicher Sicht kann man dieses Risiko durchaus hinnehmen, weil sich Zusatzwissen im Einzelfall nicht verhindern lässt. Die datenschutzrechtliche Zulässigkeit war damit nicht gefährdet.

4. Datenschutz im MDR

4.6 HbbTV und Datenschutz

In meinem letzten Bericht für den Zeitraum 2013 bis 2014 hatte ich ausführlich über datenschutzrechtliche Fragestellungen im Zusammenhang mit HbbTV-Angeboten berichtet. HbbTV (Hybrid Broadcast Broadband TV) wird der Stan-

dard genannt, der es ermöglicht, dass parallel zum laufenden Fernsehprogramm zusätzliche Webinhalte durch die Sender angezeigt werden können. Ich hatte beschrieben, dass hierbei die IP-Adresse übertragen werden muss und diese als personenbezogenes Datum schutzwürdig ist.

Das Problem besteht insbesondere darin, dass diese IP-Adresse aus technischen Gründen bereits dann übertragen wird, wenn der Sender eingeschaltet wird und bevor sich der Nutzer dazu entscheidet, dieses zusätzliche Webangebot tatsächlich zu nutzen. Diese Entscheidung erfolgt grundsätzlich durch das Drücken des „Red-Button", womit der Abruf des jeweiligen Telemediendienstes bewusst veranlasst wird. In enger Zusammenarbeit mit der Kollegin vom RBB habe ich mich mit der datenschutzgerechten Gestaltung des Angebotes für die ARD-Startleiste, die vom Playoutcenter in Potsdam zu verantworten ist, befasst. Wir haben eine sehr ausführliche Datenschutzerklärung gestaltet, die insbesondere das Abwählen der (anonymen) Nutzungsmessung auf einfache Weise veranschaulicht und damit ermöglicht. In Berlin und Brandenburg gibt es die sog. geteilte Zuständigkeit beim Datenschutz, so dass auch die staatlichen Datenschützer dort an der Thematik mitgearbeitet haben. Ausdrücklich gelobt wurde unsere transparente Aufklärung zum Datenschutz, jedoch hat es einiger Überzeugungsarbeit bedurft, sich mit den staatlichen Datenschützern darüber zu verständigen, die IP-Adresse bereits vor Drücken des „Red-Button" zu übertragen. Richtigerweise wurde darauf hingewiesen, dass allein die Nutzung des TV-Programms nicht ausreicht, um die Datenverarbeitung zu rechtfertigen. Wir haben uns daher darauf geeinigt, dass die vor der Betätigung des „Red-Button" im Zusammenhang mit dem Einschalten eines HBBTV-Senders übertragene Daten nicht für die Bildung von Nutzungsprofilen verwendet werden. Somit werden die personenbezogenen Daten vor aktiver Nutzung des Webangebotes allein für technische Zwecke genutzt, nicht jedoch, um in irgendeiner Form Nutzungsmessungen vorzunehmen. Dies ermöglicht es, die datenschutzrechtlichen Belange mit einer nutzerfreundlichen Ausgestaltung der Angebote in Einklang zu bringen. Langfristig wäre es natürlich wünschenswert, wenn jeglicher Kontakt mit dem Internet erst dann aufgebaut würde, wenn der Nutzer sich bewusst für die Aktivierung eines Webangebotes entscheidet. An diesem Thema wird weiter gearbeitet, damit

technisch ein vollkommen anonymes Fernsehen auch im Zeitalter der Smart TVs möglich sein wird.

4. Datenschutz im MDR

4.7 Multimediale Produktions-App

Die multimediale Produktions-App (MuPro-App) der ARD ist eine Software, die auf einem Smartphone oder einem Laptop installiert werden kann. Damit macht sie diese Geräte zu universellen Produktionsmitteln für Reporter. Es können O-Töne und Interviews aufgezeichnet werden, es können erste Beiträge am Ort des Geschehens produziert und unverzüglich per Filetransfer der ARD oder einzelnen Programmen überspielt werden. Mit dieser App kann vom Reporter zur Verfügung gestelltes Material an einen Server im ARD-Sternpunkt übermittelt und von dort an die sendenden Rundfunkanstalten weitergeleitet werden. Zunächst werden die Audiofunktionalitäten genutzt, erst in einem zweiten Schritt können dann die Videofunktionalitäten hinzukommen. Personenbezogene Daten werden bei dieser Software ausschließlich zu journalistischen Zwecken verwendet. Aufgrund der Tatsache, dass für journalistische Datenverarbeitung das Datenschutzrecht nur eingeschränkt gilt und insbesondere keine Einwilligung der Betroffenen oder eine sonstige gesetzliche Grundlage erforderlich ist, war das Ergebnis klar: die Datenverarbeitung mit Hilfe der MuPro-App ist datenschutzrechtlich zulässig.

Allerdings muss auch hierbei beachtet werden, dass sowohl Datensicherung als auch Datengeheimnis beachtet werden.

Im Hinblick auf das Datengeheimnis ist daher sicherzustellen, dass diese Software tatsächlich nur für journalistische Zwecke verwendet wird. Dies ist organisatorisch zu lösen. Der Reporter hat im Rahmen der journalistischen Sorgfaltspflicht dafür Sorge zu tragen, dass kein unbefugter Dritter an die Daten gelangen kann.

Zentrales Augenmerk musste jedoch auf die datensicherheitstechnische Seite der App gerichtet werden. Zunächst war festzustellen, dass die mit Hilfe der MuPro-App gespeicherten und übersandten Daten nicht über Fremdfirmen verarbeitet werden. Insofern entfiel die Notwendigkeit, einen Vertrag über eine Auftragsdatenverarbeitung zu schließen. Aus technischer Sicht wird die IP-basierte Übertragung der Daten in die einzelnen Rundfunkanstalten zentral über den ARD-Sternpunkt vorgenommen. Die dort implementierten Sicherheitsmaßnahmen zur Gewährleistung einer sicheren Übertragung sowie zur Absicherung des ARD-Netzes gegen das Internet wurden bereits im Jahr 2011 sowohl von externen Dienstleistern als auch vom ARD-internen IT-Sicherheitsgremium geprüft. Der sichere Zugang der App-Nutzer zur Infrastruktur wird durch Verwendung eines verschlüsselten Passwortes bei der Registrierung des Gerätes gewährleistet. Die Verschlüsselung der tatsächlichen Audioübertragung wird von den Endgeräteherstellern noch nicht unterstützt. Daher wird an dem Thema der Komplettverschlüsselung weiter gearbeitet.

Beim MDR wird die multimediale Produktions-App lediglich auf MDR-eigenen Geräten installiert. Diese Geräte werden zu dienstlichen Zwecken an die festangestellten oder freien Mitarbeiterinnen und Mitarbeiter ausgegeben. Die Steuerung dieser Geräte erfolgt ausschließlich über das sog. Mobile Device Management System des MDR und folgt den für den Betrieb vereinbarten Regelsätzen. Damit ist gewährleistet, dass die IT-Sicherheit gemäß den Vorgaben des MDR eingehalten wird. Wesentlicher Bestandteil ist das Fernlöschen der Geräte bei Verlust und die Pflichtaktivierung eines sechsstelligen Gerätepins. Aus datensicherheitstechnischer Sicht wäre es hingegen nicht ganz so einfach, wenn die MuPro-App auf Privatgeräten der Journalisten installiert werden dürfte. Hier stellten sich andere sicherheitstechnische Fragen, die einer gesonderten Bewertung vorbehalten sind.

Im Ergebnis konnte ich damit der MuPro-App die datenschutzrechtliche Freigabe erteilen.

4. Datenschutz im MDR

4.8 Kaisermania

Als „Kaisermania“ wird ein großes Konzert von Roland Kaiser in Dresden bezeichnet, das jedes Jahr sehr viele Menschen mobilisiert. Im Rahmen der Kaisermania 2015 sollte bei MDR.de die Möglichkeit vorgesehen werden, dass die Fans Roland Kaiser Nachrichten per WhatsApp schicken können. Ausgewählte Nachrichten sollten während der Live-Sendung eingeblendet werden. Hier stellte sich nun die Frage nach der datenschutzrechtlichen Zulässigkeit.

Ich habe zunächst darauf abgestellt, dass eine solche Einblendung nur mit der Einwilligung des jeweils Betroffenen zulässig ist. Die Menschen sind zuvor über die beabsichtigte Veröffentlichung, also über die Verarbeitung Ihrer Daten aufzuklären. Die im Gesetz eigentlich vorgesehene Schriftlichkeit ist in einem solchen Fall natürlich unrealistisch, so dass in Ausnahmefällen von diesem Erfordernis abgewichen werden kann, wenn es die Umstände erfordern. Ich habe die Auffassung vertreten, dass in diesem Fall besondere Umstände vorliegen und deshalb besonderes Augenmerk auf die Aufklärung im Vorfeld gelegt werden muss. Außerdem habe ich empfohlen, Nachrichten tatsächlich nur mit einem Nickname oder mit dem Vornamen des Teilnehmers zu veröffentlichen. Hierdurch wird eine Identifikation des Teilnehmers erschwert, trotzdem kann er sich über die Veröffentlichung seiner Nachricht freuen. Ebenso habe ich darauf hingewiesen, dass im Rahmen dieser Aktion nicht für die Installation des Messengers WhatsApp „geworben“ werden sollte. Die Nutzung dieses Dienstes ist zwar mittlerweile sehr verbreitet, jedoch sollte der MDR im Hinblick darauf, dass der Datenschutz bei WhatsApp häufig angezweifelt wird, nicht auch noch für diesen Messenger Werbung machen. Insgesamt war mir wichtig, dass sowohl den datenschutzrechtlichen Belangen große Aufmerksamkeit gewidmet wird und nicht in unbedachter Form mit den Daten der Nutzer umgegangen wird, jedoch auch eine professionelle Produktion nicht unnötig behindert wird. Ich glaube in diesem Fall ist dies in zufriedenstellender Weise gelungen.

4. Datenschutz im MDR

4.9 Personennotrufsystem

Im Bereich der technischen Infrastruktur müssen Arbeiten an elektrischen Anlagen ausgeführt werden. Diese Arbeiten sollen laut Sicherheitsrichtlinie nicht allein ausgeführt werden, dies kann aber aus betrieblichen Gründen ausnahmsweise notwendig sein, etwa wenn Mitarbeiter in der Spätschicht oder in der Bereitschaft allein im Haus sind. Ist dies der Fall, müssen Maßnahmen zur Personensicherheit ergriffen werden. Ich wurde zu diesem Thema befragt, weil ein Personennotrufsystem so schnell wie möglich das Auffinden und die Rettung des verunglückten Mitarbeiters gewährleisten muss und es deshalb erforderlich ist, dass Daten dieses Mitarbeiters genutzt werden.

Zunächst einmal war sicherzustellen, dass mit diesem System keine Leistungs- und Verhaltenskontrolle einhergeht. Dieses Notrufgerät kann nämlich im täglichen Betrieb ohne Alarmfunktion als Telefon genutzt werden. Wenn die Alarmfunktion benötigt wird, muss diese im Gerät selbst aktiviert werden, so dass die Übermittlung des Standortes nur im Ausnahmefall möglich ist.

Aus datenschutzrechtlicher Sicht interessant ist überdies, dass mit diesem Notrufsystem eine Fremdfirma beauftragt werden soll. Werden also personenbezogene Daten an einen Dritten außerhalb des MDR weitergegeben, muss ein spezieller Vertrag geschlossen werden, eine sog. Vereinbarung über die Auftragsdatenverarbeitung. Im Falle eines Alarms wird die Position des Funktelefons per GPS ermittelt und an eine ständig besetzte Leitstelle weitergeleitet. Diese Leitstelle wird von einer Fremdfirma bereitgestellt. Diese Leitstelle informiert den MDR, der dann die Hilfe organisieren muss.

Zunächst mal war für mich fraglich, ob allein die Position des Funktelefons ein personenbezogenes Datum darstellt. Im Zusammenhang mit der Identität des nutzenden Mitarbeiters ist dies selbstverständlich der Fall. Allerdings wurde in der Diskussion deutlich, dass die Identität des jeweiligen MDR-Mitarbeiters der Fremdfirma, die den Notruf erhält, nicht bekannt sein muss. Es reicht die Positi-

on des Funktelefons und die Information, dass ein Notfall vorliegt. Die Identität der verunfallten Person muss in der Leitstelle nicht bekannt sein. Erst beim MDR können die Daten insoweit zusammengeführt werden. Daher konnte eine datenschutzrechtliche saubere Lösung gefunden werden, die ohne eine Weiterleitung von persönlichen Daten von Mitarbeitern an eine Fremdfirma auskommt. Aus datenschutzrechtlicher Sicht ist dies auch deswegen zu begrüßen, weil ebenso die Grundsätze der Datenvermeidung und Datensparsamkeit beachtet wurden. Es konnte also ein System bereitgestellt werden, die sowohl den Sicherheitsbedürfnissen als auch dem Datenschutz Rechnung trägt.

4. Datenschutz im MDR

4.10 Erneuerung der Telekommunikationsanlage

Der MDR hat seine Telekommunikationsanlage erneuert. Um mit der Zeit zu gehen, wurde für einen Teil der Telekommunikationsteilnehmer eine sog. Unified Communication (UC) Lösung eingeführt. Diese Lösung bietet moderne Kommunikationsmöglichkeiten am Arbeitsplatz, ggf. in Besprechungsräumen und auch mobil. Es gibt z. B. Audio- und Videokonferenzen, Instant Messaging, Präsentieren und gemeinsames zeitgleiches Bearbeiten von Dokumenten und vieles mehr. Die Telekommunikationsanlage wurde darüber hinaus mit verschiedenen anderen neuen Komponenten ausgerüstet.

Zum 01.01.2016 ist eine neue Dienstvereinbarung über Telekommunikationsanlagen in Kraft getreten, die sich unter anderem mit der Datenverarbeitung im Zuge der Nutzung der Kommunikationsanlagen beschäftigt. An der Neufassung dieser Dienstvereinbarung habe ich mitgewirkt und darauf geachtet, dass die datenschutzrechtlichen Bestimmungen berücksichtigt werden.

Im Rahmen einer Vorabkontrolle habe ich sowohl das Teilprojekt UC als auch das Teilprojekt TK-Anlage untersucht. Hier ging es insbesondere um die Frage, ob die anfallenden Daten in rechtmäßiger Weise verarbeitet werden und mit der Dienstvereinbarung im Einklang stehen. Ausführliche Zuarbeiten, für die ich an

dieser Stelle auch große Anerkennung aussprechen möchte, haben es mir ermöglicht nachzuvollziehen, in welchen Komponenten der gesamten Anlage welche Daten verarbeitet werden. Hier wurde genau beschrieben, welche Daten für die Aufrechterhaltung der Funktionalitäten erforderlich sind und wie diese vorgehalten und gespeichert werden.

Insgesamt konnte ich daher mit Unterstützung des Referates IT-Sicherheit die datenschutzrechtliche Freigabe für die Erneuerung der Telekommunikationsanlage erklären. Sowohl das Teilprojekt UC als auch das Teilprojekt TK-Anlagen entsprechend den Anforderungen.

4. Datenschutz im MDR

4.11 ARD-Box

Im gesamten MDR und auch auf ARD-Ebene ist es sehr wichtig, Daten sicher und komfortabel austauschen zu können. Jeder weiß, dass dies mit der Dropbox grundsätzlich gut möglich ist. Jedoch handelt es sich hierbei um eine sogenannte Cloud-Anwendung mit der Folge, dass die Daten irgendwo weltweit gespeichert werden. Damit kann Sicherheit und Vertraulichkeit der Daten nicht garantiert werden. Dennoch wurde dieser Dienst genutzt, einfach um den Anforderungen an Kommunikation und Workflow genügen zu können.

Um dieses Problem zu lösen und gleichzeitig die Anforderungen des Datenschutzes und der Datensicherheit zu erfüllen, wurde die ARD-Box entwickelt. Dies ermöglicht einen sichereren und unkomplizierten Austausch von Dateien mit Kollegen und Dienstleistern innerhalb und außerhalb des Mitteldeutschen Rundfunks. Die Besonderheit bei dieser Box ist, dass die Daten auf den Servern des IVZ (Informationsverarbeitungszentrum der ARD) gespeichert werden und damit dem Zugriff von Dritten garantiert entzogen sind. Es werden also die Vorteile eines Cloud-Dienstes mit der Sicherheit eines bekannten Speicherortes verbunden.

Im Gegensatz zum gängigen Austausch per E-Mail (der auch Unsicherheiten beinhaltet) können bei der ARD-Box auch sehr große Dateien ausgetauscht werden. Der Zugang ist sehr leicht zu beantragen und die Handhabung entspricht im Wesentlichen den gängigen Marktangeboten. Die ARD-Datenschützer haben an der Ausgestaltung mitgewirkt und freuen sich, dass es nunmehr ein sicheres und datenschutzgerechtes Angebot gibt, das den Anforderungen aller Beteiligten entspricht.

5. Datenschutz beim KiKA

5.1 Zusammenarbeit mit dem KiKA

Als Datenschutzbeauftragter des MDR bin ich gemeinsam mit der Datenschutzbeauftragten des ZDF für den Datenschutz beim KiKA zuständig. In unregelmäßigen Abständen findet ein Austausch zum Thema Datenschutz mit den Verantwortlichen des Kinderkanals in Erfurt statt. Hier werden Themen der aktuellen Rechtsentwicklung angesprochen, die den KiKA betreffen können.

Es wurde im Berichtszeitraum unter anderem darüber gesprochen, dass im Hinblick auf die bereits abgewiesene Klage wegen eines KiKA-Gewinnspiels (siehe vergangenen Bericht, Kapitel 5.2) neue Risiken bestehen, weil die Verbraucherschutzzentralen nunmehr aufgrund eines neuen Gesetzes wegen Datenschutzverstößen klagen könnten. Insofern muss gerade bei Gewinnspielen darauf geachtet werden, dass möglichst wenige Daten von Kindern erhoben und verarbeitete werden. Dem ist damit Rechnung getragen, dass neben einem Nickname lediglich die E-Mailadresse verwendet werden soll.

Diskutiert wurde mit dem KiKA auch die Frage, wie man die KiKA-Community ausbauen und gleichzeitig datenschutzgerecht gestalten könnte, hier spielt es eine entscheidende Rolle, dass die Daten sicher vorgehalten werden und die Eltern eng in die Prozesse einbezogen werden.

Am Ende des Berichtszeitraums wurden überdies die Datenschutzseiten von KiKA.de und der Bereich für die Eltern neu gestaltet.

Insgesamt erweist sich die Zusammenarbeit mit dem Kinderkanal samt der sehr guten Unterstützung des betrieblichen Datenschutzbeauftragten des KiKA, Jörn Voss, als fruchtbar und unkompliziert.

5. Datenschutz beim KiKA

5.2 Weiterentwicklung des Kinderdatenschutzes

In meinem letzten Bericht hatte ich unter Pkt. 5.1 zur Unterarbeitsgruppe Datenschutz bei Kindern und Jugendlichen berichtet. Das Problem besteht nach wie vor darin, dass eine isolierte Ansprache von Kindern im Netz, die auch zum Mitmachen anregen soll, ohne dokumentierte Einwilligung der Eltern rechtlich problematisch ist. Im Sommer 2015 fand ein Treffen mit dem Thüringer Datenschutzbeauftragten, Herrn Dr. Lutz Hasse, statt, um Möglichkeiten der Zusammenarbeit auszuloten. An diesem Treffen haben seitens der Rundfunkanstalten Herr Christoph Bach, Datenschutzbeauftragter des ZDF, der betriebliche Datenschutzbeauftragte des KiKA, Herr Jörn Voss sowie ich selbst teilgenommen. Die Hoffnung war, dass die Ansprache und damit verbundene Datenverarbeitung von Kindern und Jugendlichen im Netz diskutiert werden könnte, weil Herr Dr. Hasse das Thema Medienkompetenz im Kreis der Landesdatenschutzbeauftragten federführend betreut. Das Gespräch brachte insoweit jedoch keinen Ertrag, da das Interesse Herrn Dr. Hasses vor allen Dingen darin bestand, wie man das Thema Medienkompetenz auch im Rahmen des KiKA-Programmangebots vorantreiben könne, was aber eher eine redaktionelle Frage und weniger eine datenschutzrechtliche Problematik ist. Dennoch wurde deutlich, dass der KiKA gute Ansätze hinsichtlich des Kinderdatenschutzes verfolgt.

In diesem Zusammenhang sollte nicht unerwähnt bleiben, dass am 14.04.2016 die EU-Datenschutzgrundverordnung in Kraft gesetzt worden ist (siehe auch Kapitel 3.1 dieses Berichtes). Nach Art. 8 dieser Verordnung ist die Verarbeitung

der personenbezogenen Daten eines Kindes rechtmäßig, wenn es das 16. Lebensjahr vollendet hat. Die Mitgliedsstaaten dürfen gem. einer sog. Öffnungsklausel vorsehen, dass die Altersgrenze bis 13 Jahre herabgesetzt wird. Ebenfalls in dieser Vorschrift ist festgelegt, dass die verantwortliche Stelle angemessene Anstrengungen unternimmt, um sich zu vergewissern, dass die Einwilligung erteilt worden ist. Hier wird sich in Zukunft weisen, wie diese Anforderung technisch umzusetzen ist. In den Erwägungen zu dem Gesetz ist überdies festgelegt, dass die Einwilligung der Träger der elterlichen Verantwortung im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein sollen. In diesem Kontext wird genau zu prüfen sein, inwieweit die Angebote des KiKA diesen Anforderungen entsprechen. Hier ergeben sich aus Sicht der Datenschutzbeauftragten durchaus Möglichkeiten, wie in Zukunft noch klarere Abgrenzungen und damit noch rechtssicherere Angebote erstellt werden können.

5. Datenschutz beim KiKA

5.3 Laptopverlust beim Kinderkanal

Im Herbst 2015 musste ich einem schwerwiegenden Verdacht nachgehen. Ich wurde darüber informiert, dass einem Mitarbeiter einer Firma, die für den Kinderkanal eine Struktur- und Prozessanalyse durchführt, ein Laptop mit möglicherweise sensiblen Daten des KiKA abhandengekommen sei.

Gemeinsam mit Mitarbeitern der Personalabteilung des MDR sowie der Abteilung IT-Sicherheit wurden bei dem zuständigen und verantwortlichen Dienstleister die genauen Umstände der Tat sowie die auf dem Laptop gespeicherten Daten erfragt. Auch war von Interesse, welche Maßnahmen sofort eingeleitet worden waren, ob Strafanzeige gestellt worden war und ob der Laptop und die darauf befindlichen Daten vor fremden Zugriff besonders geschützt waren.

Es stellte sich heraus, dass sich der Laptop in einer Fahrradtasche befunden hatte und der Mitarbeiter diese unbeaufsichtigt zurückgelassen hatte, während er sein

Kind vom Kindergarten abholte. Glücklicherweise konnte genau rekonstruiert werden, welche Daten auf dem Laptop gespeichert waren. Es handelte sich um anonyme und aggregierte Daten, die keinen Personenbezug aufwiesen. Dies erwies sich nach Rücksprache mit den Verantwortlichen des Kinderkanals als nachvollziehbar, weshalb dieser zunächst als sehr kritisch eingestufte Vorfall aus datenschutzrechtlicher Sicht nicht mehr problematisch war.

Dennoch muss festgehalten werden, dass die Risiken eines Datenverlustes nicht von der Hand zu weisen sind und stets in sehr sorgfältiger Weise auf die Aspekte der Datensicherheit geachtet werden sollte. Gut gelungen ist in diesem Fall die schnelle Abstimmung innerhalb des Hauses und zu loben ist ebenso die reibungslose Zusammenarbeit mit der Hauptabteilung Personal und Organisationsentwicklung und der Abteilung IT-Sicherheit.

6. Datenschutz beim Beitragsservice

6.1 Datenschutz im Zusammenhang mit dem Rundfunkbeitrag

Die Datenschutzbeauftragten der einzelnen Rundfunkanstalten sind für die Überwachung des Datenschutzes bei der Verarbeitung von Rundfunkteilnehmerdaten zuständig. Direkte Berührung mit den Teilnehmern haben die Datenschutzbeauftragten meistens dann, wenn Eingaben und Auskunftsersuchen von Teilnehmern direkt bei ihnen eingehen. Diese werden, sofern keine Besonderheiten ersichtlich sind, beim MDR direkt von der Abteilung Beitragsservice beantwortet. Meistens handelt es sich lediglich um die Frage zu den gespeicherten und verarbeiteten Daten. Wenn es datenschutzrechtlich schwierigere Fragen gibt, antworte ich zumeist selbst. Immer wird Auskunft über die gespeicherten Daten gegeben und erläutert, auf welcher Rechtsgrundlage (Rundfunkbeitragsstaatsvertrag) die Daten erhoben und verarbeitet werden. Zudem wird stets auf die strenge Zweckbindung verwiesen, nach der die Daten ausschließlich zum Zwecke des Beitragseinzuges verwendet werden dürfen.

Im Berichtszeitraum haben mich persönlich 48 Anfragen erreicht, die hauptsächlich von der Abteilung Beitragsservice beantwortet werden konnten.

6. Datenschutz beim Beitragsservice

6.2 Evaluierung des Rundfunkbeitragsstaatsvertrages

Ab dem 01.01.2013 gilt der Rundfunkbeitragsstaatsvertrag, der den Rundfunkgebührenstaatsvertrag abgelöst hat. Die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio haben auch die Frage diskutiert, inwieweit der Staatsvertrag sich auch aus datenschutzrechtlicher Sicht bewährt hat und welche Änderungen ggf. vorgenommen werden könnten. Bereits im September 2014 wurde diese Frage im Rahmen der Sitzung des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio diskutiert. Hier wurde über die Frage gesprochen, ob auch in Zukunft auf den Ankauf und die Anmietung von Adressdaten verzichtet werden könne und stattdessen der zunächst einmalige Meldedatenabgleich in regelmäßigen Abständen wiederholt werden könnte. Den Datenschutzbeauftragten erschien dies als sinnvolles Mittel, um den sehr aufwändigen Adressdatenankauf zu vermeiden und den Datenbestand aktuell und möglichst korrekt zu halten.

Sodann wurde darüber gesprochen, inwieweit auch E-Mail-Adressen und Telefonnummern beim Beitragseinzug verwendet werden dürfen. Zurzeit sieht die staatsvertragliche Regelung diese Datenverarbeitung nicht vor, so dass gerade im privaten Bereich dies auch nicht möglich ist. Die Datenschutzbeauftragten haben sich dafür ausgesprochen, lediglich im nicht privaten Bereich den Kommunikationsweg über Telefon und E-Mail zu eröffnen.

Diese Auffassungen sind eingeflossen in die Stellungnahme der Datenschutzbeauftragten zum19. Rundfunkänderungsstaatsvertrag.

6. Datenschutz beim Beitragsservice

6.2 Beauftragte für den Datenschutz beim Beitragsservice

Beim Beitragsservice von ARD, ZDF und Deutschlandradio mit Sitz in Köln ist eine 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. Ihr regelmäßiger Tätigkeitsbericht ist stets von großer Sachkenntnis und Ausführlichkeit geprägt. Zudem erstattet sie regelmäßig Bericht über die Situation des Datenschutzes bei dieser Gemeinschaftseinrichtung im Rahmen des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio. Datenschutzrechtliche Vorfälle, die einer gesonderten Aufmerksamkeit der Datenschutzbeauftragten der Landesrundfunkanstalten bedurft hätten, gab es im Berichtszeitraum nicht.

7. Externe Prüfungen

Informationsverarbeitungszentraum (IVZ)

Das Informationsverarbeitungszentrum (IVZ) wird beim Rundfunk Berlin-Brandenburg (RBB) als Gemeinschaftseinrichtung des Deutschlandradios, des MDR, des NDR, des RB, des RBB, des SR und des WDR betrieben. Für die beteiligten Anstalten werden dort zentral verschiedene Aufgaben der elektronischen Datenverarbeitung abgewickelt. Im Berichtszeitraum fanden die jährlichen Treffen der beteiligten Datenschützer am 25.11.2014 und am 01.12.2015 jeweils in Berlin statt. Seitens des IVZ wurde ausführlich über datenschutzrechtliche Fragen und Entwicklungen informiert. Unter anderem wurde über den Nutzungsstand der ARD-Box berichtet. Hierbei handelt es sich um eine ARD-interne Cloud-Lösung, die entsprechende Funktionen zu dem kommerziellen Angebot Dropbox bietet (siehe dazu Kapitel 4.10 dieses Berichtes). Auch wurden Sicherheitsvorfälle im IVZ besprochen, es gab jedoch keinerlei Probleme, die ein Tätigwerden der Datenschutzbeauftragten erfordert hätten.

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

Die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio arbeiten zusammen im Arbeitskreis der Rundfunkdatenschutzbeauftragten (AK DSB). Gemeinsam mit den betrieblichen Datenschutzbeauftragten des Zentralen Beitragsservice in Köln sowie des Kinderkanals in Erfurt werden dort die Datenschutzaufgaben in dem bereits seit 1979 bestehenden Arbeitskreis koordiniert. Ziel ist unter anderem, Erfahrungen und Meinungen zu datenschutzrechtlichen Problemen in den Anstalten auszutauschen und den Datenschutz beim Rundfunkbeitragseinzug sowie bei Gemeinschaftsprojekten zu koordinieren. Der Arbeitskreis tagt zweimal jährlich; aktuelle oder dringliche Angelegenheiten werden nach Bedarf in Telefonschaltkonferenzen bzw. in Sondersitzungen beraten. Im AK DSB werden auch die Interessen und Meinungen bei gesetzgeberischen Aktivitäten in Medien- und Datenschutzbereich koordiniert und gebündelt.

Der Arbeitskreis trifft sich zweimal jährlich, im Berichtszeitraum am 25./26.09.2014, am 12./13.03.2015 und 24./25.09.2015 sowie am 14./15.04.2016.

Im Arbeitskreis der Datenschutzbeauftragten 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, insbesondere hinsichtlich der EU Datenschutz-Grundverordnung.
- Datenschutzrechtliche Aspekte im Rundfunkbeitragsstaatsvertrag
- Anforderungen an den Datenschutz im Beitragsservice
- Kinder- und Jugenddatenschutz
- HbbTV/Smart-TV
- Entwicklung eines Leitfadens für Datenschutz bei Telemedienangeboten
- Big Data

Auch in diesem Bericht möchte ich betonen, dass sich der Kreis der Datenschutzbeauftragten als kollegiales und hilfreiches Gremium erwiesen hat. Die lebhaften Diskussionen und der fachkundige Austausch helfen sowohl bei anstaltsspezifischen Fragestellungen als auch bei anstaltsübergreifenden Problemen. Insbesondere im Hinblick auf die immer komplizierter und unübersichtlicher werdenden Fragen im Online-Bereich, ist es von großer Wichtigkeit, dass alle verantwortlichen Stellen der Rundfunkanstalten eng zusammenarbeiten, damit eine gemeinsame Linie gefunden werden kann. Hier ist besonders die im Berichtszeitraum begonnene Arbeit am Leitfaden zu Telemedienangeboten hervorzuheben, die eine Vereinheitlichung des Datenschutzes in diesem Bereich anstrebt.

9. Schlussbemerkungen

Mit diesem Bericht schließe ich die zweite Hälfte meiner ersten Amtszeit ab. Es hat sich abermals erwiesen, dass Datenschutz ein wichtiges Thema ist, das an Bedeutung gewinnt.

Bereits in den letzten beiden Jahren meiner Amtszeit hat sich gezeigt, dass Personalisierung von Angeboten immer wichtiger wird. Die Rezipienten erwarten ein individuell zugeschnittenes Angebot und die Möglichkeit, sich ihr Programm selbst zusammenzustellen. Dies stellt sowohl die Redaktionen vor große Herausforderungen als auch den Datenschutz, denn für ein individuell zugeschnittenes Angebot werden personenbezogene Daten benötigt. Hier ist mit größter Sorgfalt vorzugehen und mit möglichst wenigen Daten zu operieren. Erste Schritte wurden bereits unternommen. Ich erwarte, dass dieses Thema in meinem nächsten Bericht großen Raum einnehmen wird. Auch im Bereich der Jugend- und Kinderangebote wird es auf individualisierte Angebote hinauslaufen. Hier müssen die Eltern sehr eng eingebunden werden und gerade bei Kinderdaten an die Datensicherheit und die Datensparsamkeit höchste Anforderungen gestellt werden.

In der nächsten Amtszeit besteht zudem eine rechtliche Unsicherheit. Durch die in Kraft getretene EU Datenschutz-Grundverordnung werden die Regelungen des Datenschutzes auf eine neue Grundlage gestellt. Dies birgt große Herausforderungen für die Anwender. Die Datenverarbeitung im MDR wird in vielen Bereichen einer datenschutzrechtlichen Neubewertung unterzogen werden müssen. Auch wird die anstaltsautonome Kontrolle des Datenschutzes zu verteidigen sein, damit auch in diesem Bereich die Staatsfreiheit gewährleistet bleibt. Hier ist der enge Schulterschluss mit den anderen Landesrundfunkanstalten von großer Bedeutung.

Festhalten kann ich, dass die Arbeit als Datenschutzbeauftragter große Freude bereitet hat und die Zusammenarbeit mit dem Haus hervorragend funktioniert. Ich darf mich daher bei allen Mitarbeiterinnen und Mitarbeitern sehr herzlich bedanken, die mich unterstützt haben und mir mit ihrer Mitarbeit das Leben erleichtert haben. Ich freue mich auf die kommende Amtsperiode und hoffe, dass das Thema Datenschutz auch weiterhin so einen hohen Stellenwert im Haus behalten wird.

10. Anhang

10.1 § 39 – 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 personengebundenen 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 §§ 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, dürften 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 Bestandsund 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:

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

stellt 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

10.3 §§ 7 bis 9 MDR-Rundfunkbeitragssatzung

§ 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 Auskunftsersuchen 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 installiert und die Löschung der Daten von Rundfunkteilnehmern und Beitragsschuldnern nach einem einheitlichen Konzept geregelt wird.

10. Anhang

10.4 Verfahrenskodex der Rundfunkbeauftragten für den Datenschutz

(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

10.5 Mitglieder des Arbeitskreises der Datenschutzbeauftragten von 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: Axel Kaufmann
Saarländischer Rundfunk	Sonnia Wüst
Südwestrundfunk	Prof. Dr. Armin Herb Referat: Marianne Gottheil
Westdeutscher Rundfunk	Karin Wagner Referat: Günter Grießbach
Zweites Deutsches Fernsehen	Dr. Frauke Pieper
Kinderkanal ARD/ZDF	Jörn Voss
Österreichischer Rundfunk	Rainer Rauch