

2. Tätigkeitsbericht

der Beauftragten für den Datenschutz
des Rundfunk Berlin-Brandenburg

Berichtszeitraum:

1. April 2004 bis 31. März 2005

Dem Rundfunkrat vorgelegt von Anke Naujock

Vorbemerkung

Auch im „Jahr 2 des **rbb**“ sind wir mit den Themen Datenschutz und Datensicherheit wieder ein ganzes Stück vorangekommen. Nach meinem Eindruck ist das Bewusstsein dafür inzwischen in allen Bereichen des Hauses verankert. So ist es z.B. zur Routine geworden, bei neuen IT-Projekten die Datenschutzbeauftragte von Anfang an mit einzubeziehen.

Dennoch bleibt auf dem Weg zum „datenschutzrechtlichen Regelbetrieb“ einiges zu tun. Nach wie vor fehlen grundlegende innerbetriebliche Regelungen zum Datenschutz, wie z.B. die Datenschutz-, PC- und Wartungsrichtlinien. Um über die gesetzlichen Vorgaben hinaus überhaupt eine Orientierung zu haben, werden die einschlägigen Richtlinien von ORB und SFB weiterhin sinngemäß angewandt.

Dieser Zustand hat im **rbb** zu einer gewissen Rechtsunsicherheit geführt. Es dürfte daher im Interesse von Datenschutz und Datensicherheit, aber auch im Interesse aller Nutzerinnen und Nutzer, aller Administratorinnen und Administratoren und aller sonstigen Verantwortlichen liegen, dass jetzt so schnell wie möglich verbindlich die Rechte und Pflichten für den Umgang mit personenbezogene Daten in den vorgenannten Richtlinien konkretisiert werden.

Auch eine konkrete gesetzliche Forderung ist im **rbb** bislang nicht umgesetzt worden: noch immer ist die in § 19 a BlnDSG vorgesehene Position eines/einer stellvertretenden behördlichen Datenschutzbeauftragten vakant.

Aus meiner Sicht sollte diese Position jetzt möglichst rasch besetzt werden. Dadurch wäre auch gewährleistet, dass es jederzeit eine/n Ansprechpartner/in für den Datenschutz im **rbb** gibt. Da ich hauptamtlich Mitarbeiterin des Justitiariats bin und ich mich daher naturgemäß im Wesentlichen um die rechtlichen Fragestellungen im Zusammenhang mit Datenschutz und Datensicherheit kümmere, hielte ich es für ideal, wenn eine Person mit technischem Background zur Stellvertreterin/ zum Stellvertreter benannt würde, um auf diese Weise auch die technische Seite, die zunehmend an Bedeutung gewinnt, mit abzudecken.

Auch in diesem Jahr möchte ich mich bei der Intendantin, den weiteren Mitgliedern der Geschäftsleitung und den sonstigen Verantwortungsträgern für das mir entgegengebrachte Vertrauen bedanken. Meinen Empfehlungen wurde auch im Berichtsjahr wieder ausnahmslos gefolgt. Dem Personalrat danke ich für die konstruktive Zusammenarbeit.

A. Die Stellung der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg

I. Gesetzliche Grundlagen

1. Rundfunkdatenschutzbeauftragte gemäß § 38 rbb-Staatsvertrag

Gemäß § 38 Abs. 1 **RBB**-Staatsvertrag bestellt der Rundfunkrat einen Beauftragten oder eine Beauftragte für den Datenschutz. Der oder die Beauftragte für den Datenschutz ist in Ausübung seines/ihrer Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er/sie der Dienstaufsicht des Verwaltungsrates.

Die Aufgaben der Rundfunkdatenschutzbeauftragten sind in § 38 Abs. 2 bis 7 geregelt. Gemäß Abs. 2 Satz 2 überwacht sie die Einhaltung der Datenschutzvorschriften des **rbb**-Staatsvertrags und anderer Vorschriften über den Datenschutz, *soweit der **rbb** personenbezogene Daten zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet*. Soweit eine Befugnis des oder der Beauftragten für den Datenschutz nach Abs. 2 Satz 1 nicht gegeben ist, obliegt die Kontrolle der Einhaltung von Datenschutzbestimmungen beim **rbb** dem Landesbeauftragten für den Datenschutz des Landes Berlin. Die Kontrolle erfolgt im Benehmen mit dem Landesbeauftragten für Datenschutz des anderen Landes (Abs. 8).

Darauf, dass diese Aufspaltung der Kontrollkompetenzen, die es vergleichbar außer beim **rbb** nur noch beim Hessischen Rundfunk und bei Radio Bremen gibt, verfassungsrechtlich zumindest bedenklich ist und in der Praxis immer wieder zu Problemen führt, bin ich in meinem 1. Tätigkeitsbericht ausführlich eingegangen (s. dort S. 3 ff). An meiner Position halte ich fest.

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

2. Behördliche Datenschutzbeauftragte gemäß § 19 a Berliner Datenschutzgesetz

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

Die Funktionen des/der Rundfunkdatenschutzbeauftragten nach § 38 Abs. 1 **rbb**-Staatsvertrag und des/der behördlichen Datenschutzbeauftragten gemäß § 19 a BlnDSG werden wegen der in der Praxis häufig vorkommenden Abgrenzungsschwierigkeiten zwischen dem journalistisch-redaktionellen und dem wirtschaftlich-administrativen Bereich zweckmäßigerweise von ein und derselben Person wahrgenommen.

II. Konkrete Situation

Auf seiner Sitzung am 26. Mai 2003 hat mich der Rundfunkrat gemäß § 38 Abs. 1 **rbb**-Staatsvertrag auf Vorschlag der Intendantin für eine Amtszeit von vier Jahren zur Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg bestellt.

Gemäß dem Beschluss der Geschäftsleitung vom 24. Juni 2003 hat mich die Intendantin für den gleichen Zeitraum auch mit der Wahrnehmung der Aufgaben der behördlichen Datenschutzbeauftragten im Sinne von § 19 a BlnDSG beauftragt. Meine Stellvertretung ist bislang nicht geregelt. In der Gründungsphase des **rbb** hatte der Mitarbeiter der Revision und ehemalige stellvertretende Datenschutzbeauftragte des SFB, Herr Eberhard Mohr, diese Aufgabe noch kommissarisch wahrgenommen; inzwischen ist er diesbezüglich nicht mehr tätig.

B. Entwicklung des Datenschutzrechts

I. Die Europäische Verfassung

Am 29. Oktober 2004 unterzeichneten die Staats- und Regierungschefs der 25 EU-Mitgliedstaaten und der drei Kandidatenländer den Vertrag über eine Verfassung für Europa, den sie am 18. Juni 2004 einstimmig angenommen hatten.

Dieser Vertrag über eine Verfassung in Europa wird in Kraft treten, wenn er von jedem Unterzeichnerstaat nach dem von dessen jeweiliger Verfassung vorgeschriebenen Verfahren ratifiziert worden ist.

Während das Deutsche Grundgesetz ein Grundrecht auf Datenschutz nicht ausdrücklich erwähnt, dieses vielmehr durch die Rechtsprechung des Bundesverfassungsgerichts erst entwickelt werden musste, nennt die Europäische Verfassung gleich mehrfach den Schutz personenbezogener Daten. Als einziges Grundrecht wird es sowohl im Teil I, der eigentlichen Verfassung (Art. 1-50), als auch in Teil II, der Charta der Grundrechte der Union (Art. II - 8), verankert.

II. Novellierung des Telekommunikationsgesetzes

Am 26. Juni 2004 ist das neue Telekommunikationsgesetz (TKG) in Kraft getreten. Es ersetzt das Telekommunikationsgesetz vom 25. Juli 1996. Die Telekommunikations-Datenschutzverordnung vom 18. Dezember 2000 wurde aufgehoben und in das TKG integriert. Datenschutzrechtlich bringt das neue Gesetz keine Verbesserungen, es führt vielmehr zu einer Absenkung des Datenschutzniveaus.

Die wesentlichen datenschutzrechtlichen Neuerungen stehen in den Vorschriften über die Datennutzung für die öffentliche Sicherheit.

Im TKG ist die Übermittlung von Daten an die Sicherheitsbehörden nur für die Bestandsdaten geregelt. Regelungen zu den Verkehrsdaten sowie den Inhalten der Telekommunikation finden sich z.B. in der Strafprozessordnung (§§ 100 a, 100 b, 100 g, 100 h).

Die Erhebungspflicht für Bestandsdaten ergibt sich aus § 111 TKG. Weil § 90 TKG-alt nach Auffassung des BVerwG nicht ausreichte, um eine Pflicht zur Speicherung der Bestandsdaten auch dann zu schaffen, wenn dies aus betrieblichen Gründen nicht erforderlich ist, hat der Gesetzgeber diese Fragestellung insgesamt neu geregelt. Bei Vertragsabschluß sind – unabhängig von der Erforderlichkeit für die Vertragsabwicklung – Name und Anschrift des Rufnummerninhabers, bei natürlichen Personen auch das Geburtsdatum und bei Festnetzanschlüssen auch der Standort des Anschlusses zu erheben. Darüber hinaus sind Vertragsbeginn, Freischaltung des Anschlusses und ggf. das Vertragsende zu erheben. Während der Vertragsabwicklung sind zudem auch Änderungen der Daten zu erfassen. Die Daten dürfen erst mit dem Ablauf des auf das Ende des Vertragsverhältnisses folgenden Kalenderjahres gelöscht werden.

Die durch den Bundestag beschlossene Ausnahme von der Pflicht zur Erhebung der Bestandsdaten für Prepaid-Produkte konnte sich im Vermittlungsausschuss nicht durchsetzen. Schon in meinem letzten Tätigkeitsbericht hatte ich darauf hingewiesen, dass diese Datenvorratsspeicherung insbesondere bei Prepaid-Produkten aus allgemeinen datenschutzrechtlichen Erwägungen abzulehnen ist. Außerdem wird den Journalistinnen und Journalisten durch die Registrierung der Prepaid-Handys ein Instrument zur Wahrung des Informantenschutzes und des Redaktionsgeheimnisses vorenthalten.

Erfreulich im Sinne der Rechtsklarheit ist es, dass sich die Verpflichtung zur Vorhaltung von technischen Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation gemäß § 110 Abs. 1 TKG von vornherein nur auf Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienste *für die Öffentlichkeit* erbracht werden, bezieht. Damit sind die ARD-Anstalten als Betreiber eines Corporate Networks nicht von dieser Vorschrift betroffen. Vor Inkrafttreten des neuen TKG war die gebotene Eingrenzung des Kreises der Verpflichteten erst in der auf der Grundlage des TKG erlassenen Telekommunikationsüberwachungsverordnung (TKÜV) erfolgt.

III. 8. Rundfunkänderungsstaatsvertrag

Durch den 8. Rundfunkänderungsstaatsvertrag ist mit Wirkung ab 1. April 2005 eine sog. „Mailingklausel“ in den Rundfunkgebührenstaatsvertrag (RGebStV) eingefügt worden. Der genaue Wortlaut des neuen § 8 Abs. 4 RGebStV lautet:

„Die zuständige Landesrundfunkanstalt oder die von ihr nach Abs. 2 beauftragte Stelle kann zur Feststellung, ob ein Rundfunkteilnehmerverhältnis vorliegt, oder im Rahmen des Einzugs der Rundfunkgebühren entsprechend § 28 des Bundesdatenschutzgesetzes personenbezogene Daten erheben, verarbeiten oder nutzen. Das Verfahren der regelmäßigen Datenübermittlung durch die Meldebehörden nach den Meldegesetzen oder Meldedatenübermittlungsverordnungen der Länder bleibt unberührt.“

Die Regelung verfolgt den Zweck, für die Rundfunkanstalten und die GEZ eine einheitliche und gesicherte Rechtsgrundlage für die Datenerhebung bei Dritten (den Adresshändlern) zu schaffen. Die Zulässigkeit der Adressanmietung durch die GEZ richtete sich bislang nach jeweils unterschiedlichen landesdatenschutzrechtlichen Regelungen, die von einigen Landesdatenschutzbeauftragten (unter anderem auch von dem Berliner und Brandenburgischen Datenschutzbeauftragten) nicht als hinreichende Rechtsgrundlage für die Praxis der GEZ angesehen wurden. Demgegenüber hatte die Rechtsaufsicht dem **rbb** auch schon in der Vergangenheit auf der Grundlage der einschlägigen landesrechtlichen Vorschriften rechtmäßiges Verhalten bestätigt.

Auch gegen die geplante Neuregelung hat sich heftiger Widerstand, u. a. des Berliner und Brandenburgischen Landesdatenschutzbeauftragten, geregt. Die Landesdatenschutzbeauftragten vertreten die Auffassung, dass § 8 Abs. 4 RGebStV mit datenschutzrechtlichen Grundsätzen nicht zu vereinbaren sei. Während öffentlich-rechtliche Institutionen personenbezogene Daten nur verarbeiten dürften, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, sei die Datenverarbeitung der im Wettbewerb stehenden Privatwirtschaft vom Prinzip der Vertragsfreiheit geprägt. Die öffentlich-rechtlichen Rundfunkanstalten stünden hinsichtlich

des Gebühreneinzugs in keinem Wettbewerb zu anderen Rundfunkveranstaltern. Eine parallele Nutzung von Daten aus den Melderegistern auf der Grundlage der Einwohnermeldedatenübermittlungsverordnungen bei gleichzeitiger Beschaffung von Adressen im privaten Adresshandel sei unverhältnismäßig. Zudem werde durch § 8 Abs. 4 das Ziel der Rundfunkanstalten nicht erreicht. Die Beschaffung von Adressen beim kommerziellen Adresshandel durch die GEZ sei rechtswidrig, da sich die Erhebung von personenbezogenen Daten bei Dritten ohne Kenntnis der Betroffenen weiterhin nach dem maßgeblichen Landesrecht richte.

Dem ist Folgendes entgegen zu halten:

Die Pflicht zur Zahlung von Rundfunkgebühren ist eine gesetzlich begründete Pflicht aller Rundfunkteilnehmerinnen und -teilnehmer. Die Rundfunkanstalten stehen vor dem Problem, dass sie einen beträchtlichen Teil der Teilnehmerinnen und Teilnehmer (= ihre Schuldner) nicht kennen. Dieses Problem dürfte, zumindest in dieser Größenordnung, einmalig für öffentliche Einrichtungen sein, deshalb rechtfertigt die besondere Sachlage hier eine problemspezifische Regelung.

Die in einigen Bundesländern, u.a. in Berlin, existierende datenschutzrechtliche Regelung, wonach personenbezogene Daten grundsätzlich nur beim Betroffenen erhoben werden dürfen, ist kein verfassungsrechtlich begründetes Dogma. Dies ergibt sich schon daraus, dass in anderen Bundesländern die Erhebung von Daten bei Dritten - und damit auch die Anmietung von Adressen bei privaten Adressanbietern - unstreitig zulässig ist.

Das auf den öffentlichen Bereich beschränkte Prinzip, Daten grundsätzlich beim Betroffenen zu erheben, dürfte seinen Grund im Wesentlichen darin haben, dass die öffentliche Hand die Daten in der Regel im Rahmen der Eingriffsverwaltung verwendet. Hier geht es hingegen um reine Informationsschreiben der GEZ, die lediglich zur freiwilligen Anmeldung von Rundfunkgeräten animieren sollen.

Weder die Landesrundfunkanstalten noch die GEZ handeln mit Adressbeständen und sie dürfen dies auch vor dem Hintergrund des neuen § 8 Abs. 4 RGebstV nicht.

Danach ist die Zweckbindung („zur Feststellung, ob ein Rundfunkteilnehmerverhältnis vorliegt, oder im Rahmen des Einzugs der Rundfunkgebühren“) eindeutig.

Ziel des § 8 Abs. 4 RGebStV ist es, neben der Gewährleistung der Chancengleichheit unter den Landesrundfunkanstalten Gebührengerechtigkeit herzustellen. Das Potential der Schwarz Hörer und -seher soll möglichst klein gehalten werden. Dies wiederum hilft, den Anstieg der Rundfunkgebühr gering zu halten. Aus dem gleichen Grund wurde vor einigen Jahren in allen Bundesländern auch die automatische Datenübermittlung von Bewegungsdaten durch die Meldebehörden an die GEZ zugelassen. Dies geschah insbesondere auf Anregung der Rechnungshöfe.

Die Beschaffung von Adressen beim privaten Adresshandel ist neben der Datenübermittlung durch die Meldebehörden erforderlich. Von den Meldebehörden erhalten die Rundfunkanstalten nur die Adressen von Personen, die umziehen oder verstorben sind. Zieht ein Rundfunkteilnehmer nicht um oder meldet er sich entgegen den bestehenden melderechtlichen Vorschriften nicht bzw. verspätet um, so kann er entweder überhaupt nicht, oder erst zu einem sehr viel späteren Zeitpunkt durch die Rundfunkgebührenbeauftragten der Landesrundfunkanstalten ermittelt werden. Mit der Ansprache der nicht gemeldeten Teilnehmer per Brief soll mit einem bürgerfreundlichen Verfahren dafür gesorgt werden, dass die Besuche von Beauftragten an den Haustüren auf ein Minimum reduziert werden können.

Ferner bezieht sich die Datenübermittlung der Einwohnermeldeämter nur auf Privatpersonen. Firmenanschriften erhalten die Rundfunkanstalten auf diesem Weg nicht, so dass sie bezüglich dieses Segments allein auf Adressanmietungen angewiesen sind. In diesem Bereich können in aller Regel datenschutzrechtliche Prinzipien ohnehin keine Anwendung finden, weil durch die Datenschutzgesetze nur natürliche Personen geschützt werden.

§ 8 Abs. 4 RGebStV, der auf § 28 BDSG verweist, ist eine abschließende Sonderregelung und geht insofern den Landesdatenschutzgesetzen vor. Er berechtigt zur Datenerhebung bei Dritten. Dafür spricht auch die Begründung der Vorschrift, die die Anmietung von Adressen bei privaten Adresshändlern ausdrücklich erwähnt.

IV. 9. Rundfunkänderungsstaatsvertrag/Telemediengesetz - TMG

Im Rahmen der nächsten Novellierung des Rundfunkstaatsvertrages ist vorgesehen, den Rundfunkstaatsvertrag in „Staatsvertrag für Rundfunk und Telemedien“ umzubenennen und wesentliche Regelungsbereiche des bisherigen Mediendienste-Staatsvertrags zu integrieren.

Der Entwurf des 9. Rundfunkänderungsstaatsvertrages definiert Telemedien als „alle elektronischen Informations- und Kommunikationsdienste, einschließlich Fernseh- und Radiotext sowie Teleshoppingkanäle, soweit sie nicht Telekommunikation nach § 3 Nr. 22 des Telekommunikationsgesetzes oder Rundfunk nach Satz 1 und Satz 2 sind“.

Parallel dazu soll es auf der Ebene des Bundes ein Artikelgesetz geben, das den Titel „Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – EIGVG)“ haben soll. Art. 1 soll das „Telemediengesetz – TMG“ sein.

Im TMG werden bestimmte rechtliche Anforderungen an die Nutzung von Telemedien (Zugangsfreiheit, Herkunftslandprinzip, Kennzeichnungspflichten, Verantwortlichkeit, Datenschutz), die bisher im Teledienstegesetz und im Mediendienste-Staatsvertrag geregelt sind, in einem einheitlichen Bundesgesetz zusammengefasst. Die inhaltlichen Anforderungen sollen in dem Staatsvertrag über Rundfunk und Telemedien geregelt werden.

Beide Gesetzesvorhaben sind Ergebnisse von Bund-/Länderarbeitsgruppen, die am 14. und 15. Februar 2005 zusammengekommen sind. Diese Neuordnung beruht auf einem Kompromiss zwischen Bund und Ländern mit dem Ziel einer grundsätzlichen Neuordnung des Ordnungsrahmens für die elektronischen Medien. In einem ersten Schritt wurde der Jugendschutz durch den Jugendmedienschutz-Staatsvertrag der Länder aus dem Jahr 2003 realisiert, der einheitliche Jugendschutzregelungen für alle elektronischen Medien, d. h. auch für den öffentlich-

rechtlichen Rundfunk enthält. Während für den Bereich Jugendschutz in Rundfunk und Telemedien insgesamt die Länder zuständig sind, soll der Datenschutz künftig in den Zuständigkeitsbereich des Bundes fallen.

In der Begleitung der Gesetzgebungsverfahren durch die öffentlich-rechtlichen Rundfunkanstalten wird darauf zu achten sein, dass dem aus Art. 5 Abs. 1 Satz 2 GG abzuleitenden Medienprivileg sowohl hinsichtlich der materiell-rechtlichen Regelungen, als auch bei der Zuordnung der Kontrollkompetenzen Rechnung getragen wird.

V. Strafprozessordnung (StPO)

Mit seinem Urteil vom 3. März 2004 – 1 B VR 2378/98, I B VR 1084/99 – hatte das Bundesverfassungsgericht festgestellt, dass die einschlägigen Vorschriften der StPO zur akustischen Wohnraumüberwachung den Vorgaben des Art. 13 Abs. 3 GG nicht hinreichend Rechnung tragen. Es hat dem Gesetzgeber aufgegeben, einen verfassungsgemäßen Zustand bis spätestens zum 30. Juni 2005 herzustellen.

Zur Umsetzung dieser Auflage hat das Bundesjustizministerium am 24. Juni 2004 einen Referentenentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt und an die Länder und Verbände zur Stellungnahme versandt. Dieser hat eine ausführliche öffentliche Debatte ausgelöst. Dabei wurde die Notwendigkeit dieses Instruments zur Strafverfolgung ebenso thematisiert wie die Frage, ob alle vom Bundesverfassungsgericht formulierten Anforderungen erfüllt seien.

Aus Sicht der Medien ist insbesondere die danach vorgesehene Einschränkung des Abhörschutzes für Journalistinnen und Journalisten zu kritisieren. Nach der bisherigen Regelung des § 100 d Abs. 3 S. 1 StPO war in den Fällen des § 53 Abs. 1 eine Maßnahme des Abhörens und Aufzeichnens des in Wohnungen nicht öffentlich gesprochenen Wortes nach § 100 c Abs. 1 Nr. 3 StPO unzulässig. Eine Einschränkung im Hinblick auf unabweisbare Bedürfnisse einer wirksamen Strafverfolgung war in dieser Regelung nicht vorgesehen.

Nach dem neuen in dem Entwurf vorgesehenen § 100 c Abs. 7 StPO-E sind in den Fällen des § 53 Abs. 1 StPO Maßnahmen des Abhörens und Aufzeichnens des in einer Wohnung nicht öffentlich gesprochenen Wortes mit technischen Mitteln sowie die Verwertung gleichwohl aus ihr gewonnener Erkenntnisse unzulässig, soweit nicht im Einzelfall unabwendbare Bedürfnisse einer wirksamen Strafverfolgung unter besonderer Beachtung des Grundsatzes der Verhältnismäßigkeit die Maßnahme und Verwertung ausnahmsweise erfordern.

Zusammen mit anderen Medienunternehmen und -verbänden haben die öffentlich-rechtlichen Rundfunkanstalten kritisiert, dass mit der vorgesehenen Neuregelung dem Informantenschutz und dem Redaktionsgeheimnis nicht in ausreichendem Maße Rechnung getragen würde. Die Ausnahmetatbestände, die eine Überwachung auch der journalistischen Recherche ermöglichen sollen, sind nicht präzise genug formuliert. In diesem Zusammenhang wurde auch daran erinnert, dass die Medienunternehmen und -Verbände seit Jahren fordern, die Ausgestaltung der Zeugnisverweigerungsrechte für Journalistinnen und Journalisten in der Strafprozessordnung systematisch einheitlich und ohne Wertungswidersprüche zu gestalten. Dies gilt nicht nur für die in diesem Referenten-Entwurf im Mittelpunkt stehenden verdeckten Ermittlungsmaßnahmen, sondern auch in besonderem Maße für Maßnahmen der Telekommunikationsüberwachung.

VI. § 201 a StGB

Am 6. August 2004 ist der neue § 201 a StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) in Kraft getreten. Während bislang lediglich die Verbreitung eines unter Verletzung des Rechts am eigenen Bild hergestellten Bildnisses strafbar war (§ 33 KunstUrhG), ist nunmehr zusätzlich bereits das Anfertigen eines Bildnisses aus dem höchstpersönlichen Lebensbereich unter Strafe gestellt.

Ziel dieser Vorschrift ist es, die sog. „Spannerpraktiken“, also Fälle, in denen Personen Kameraaugen an versteckter Stelle, etwa in Hotelzimmern, Toiletten oder Um-

kleidekabinen installieren, um in die Intimsphäre Dritter einzudringen, zu inkriminieren.

Dass es gegen diese Praktiken nunmehr einen wirksamen strafrechtlichen Schutz gibt, ist sicherlich ein Fortschritt. Allerdings wirkt sich das neue Gesetz möglicherweise auch auf die Arbeit der Medien aus: Betroffen ist vor allem der investigative Journalismus. Drehaufnahmen aus dem höchstpersönlichen Lebensbereich, die in der Vergangenheit zur Aufdeckung von Missständen geführt haben (z.B. Missbrauch von Kindern), sind künftig möglicherweise unzulässig.

Die Vorverlagerung des strafrechtlichen Risikos stellt insbesondere an die Reporter und Kameraleute bei den Dreharbeiten hohe Anforderungen: Während sie bislang sämtliche für einen Beitrag möglicherweise interessanten Bilder zunächst einmal sammeln konnten, um dann anschließend zu entscheiden, welche Bilder tatsächlich gesendet werden können, müssen zukünftig schon beim Drehen vor Ort unter Umständen in Sekundenschnelle juristische Überlegungen zur Zulässigkeit der Bildaufnahmen angestellt werden.

Zusammen mit anderen Medienverbänden hatten sich ARD und ZDF daher bis zuletzt gegen das Gesetz in der jetzt verabschiedeten Fassung gewandt und für die Aufnahme wenigstens eines ausdrücklichen Rechtfertigungstatbestandes für die Medien in das Gesetz plädiert. Die Bemühungen blieben leider vergeblich.

Inwieweit das Gesetz die journalistische Arbeit zukünftig tatsächlich konkret behindert, lässt sich zurzeit vor allem wegen der unbestimmten Rechtsbegriffe in der Vorschrift schwer einschätzen. Es wird entscheidend auf die Rechtsprechung zu § 201 a StGB ankommen. Dabei bleibt für die Fernsehmacher zu hoffen, dass die Gerichte die Rundfunkfreiheit bei der Auslegung des Gesetzes angemessen berücksichtigen.

C. Datenschutz und Datensicherheit im rbb

I. Aktuelle IT-Projekte

1. Regelbetrieb der Groupware Lotus Notes

Nach einem mehrwöchigen Probetrieb konnte Ende 2004 damit begonnen werden, alle bisher im Hause eingesetzten E-Mail und Kalenderprogramme durch die einheitliche Groupware-Lösung Lotus Notes von IBM abzulösen. Meine Vorabkontrolle hatte zum Ergebnis, dass Lotus Notes im **rbb** ohne gravierende Änderungen und Einschränkungen eingesetzt werden kann. Dies gilt insbesondere für das umfassende Sicherheitssystem. Die beim **rbb** zum Einsatz kommenden Komponenten sind:

- E-Mail zum Verfassen, Empfangen und Weiterleiten elektronischer Mitteilungen. Diese können verwaltet, abgelegt und archiviert werden. Es können Ordner erstellt, Vorlagen angefertigt und verwendet werden.
- Der Kalender von Lotus- Notes mit Funktionen, um Besprechungen zu planen und Termine zu verwalten sowie Erinnerungen zu erstellen.
- Adressbücher zur Verwaltung öffentlicher und privater Kontakte sowie zur Erstellung von Gruppen.
- Teamroom-Anwendung, die das gemeinsame Nutzen der Funktionen von Lotus Notes erlaubt. Ein Team kann in einem gemeinsamen Arbeitsbereich arbeiten und gemeinsame Daten nutzen.

Der Betrieb von Lotus Notes erfolgt gemäß der in Zusammenarbeit mit mir erarbeiteten „**Richtlinien für die Nutzung von Lotus Notes**“ und den „**Richtlinien für die Nutzung von Internet und E-Mail**“.

In den Richtlinien für die Nutzung von Lotus Notes werden die beim **rbb** eingesetzten Komponenten beschrieben. Außerdem wird darin das Verfahren für die Vergabe von Nutzerberechtigungen und die Nutzung im Einzelnen geregelt. Aus datenschutzrechtlicher Sicht hervorzuheben ist insbesondere das differenzierte System zur Freigabe einzelner Kalendereinträge. Ausdrücklich ist festgehalten, dass Vorgesetzte nicht befugt sind, ihre Mitarbeiterinnen und Mitarbeiter zur Freigabe von persönlichen Mail- und Kalenderinformationen zu verpflichten.

Die „Richtlinien für die Nutzung von Internet und E-Mail“ regeln Verfahren für die Beantragung der Freischaltung von Diensten, die Modalitäten der Nutzung von E-Mail und der anderen, über das Internet laufenden Dienste und die Einrichtung von Schutzsystemen gegen sog. Malware und Spam sowie die zulässigen Protokollierungen.

2. SAP-Releasewechsel von Stand 4.5 nach 4.7 (Enterprise)

Zum November 2004 wurde ein SAP-Releasewechsel von Stand 4.5 nach 4.7 (Enterprise) durchgeführt. Bei dem Relasewechsel handelte es sich um eine 1:1-Migration. Alle bestehenden Funktionalitäten und Datenstrukturen wurden unverändert in das neue System übernommen. Neue Funktionen wurden nur insoweit eingerichtet, als sie für den Betrieb unter Enterprise zwingend notwendig waren.

In dem neuen System werden keine zusätzlichen personenbezogenen Daten verarbeitet. Die bestehenden Infotypen sind unverändert geblieben. Das gleiche gilt für Auswertungen mit personenbezogenen Daten, der Verarbeitung der Nutzerdaten und den Datenübermittlungen bzw. Schnittstellen.

Auch am Nutzer- und Berechtigungskonzept hat sich nichts Grundsätzliches geändert. Sowohl die Ziele und Zuständigkeiten, als auch das Verfahren der Berechtigungsvergabe sind unverändert geblieben. Die wesentliche Neuerung bei der Vergabe von Berechtigungen ist, dass die bisherigen tätigkeitsbezogenen Aktivitätsgruppen, aus denen die Benutzerprofile gebildet wurden, nunmehr in sog. Rollen zusammengefasst sind und damit die Profile arbeitsplatzbezogen gestaltet werden können. Gleichzeitig steuern die Rollen die individuelle Menüanzeige, d.h. Funktionen, für die keine Berechtigungen vergeben wurden, werden nicht angezeigt. Das überarbeitete Berechtigungskonzept, das Verfahren der Berechtigungsvergabe sowie die aktuelle Zuordnung der Berechtigungen pro Nutzer/in sind mit mir abgestimmt worden.

3. Umstieg auf das Betriebssystem Windows XP SP2

Schon seit Anfang 2003 wurden beim **rbb** vereinzelt Windows-XP-Clients ausgeliefert, da bestimmte Produktions-Software dies als Installationsbasis erfordert. Da an den einzelnen Standorten des **rbb** nach der Fusion diverse Betriebssysteme auf den Arbeitsplatz-PC vorzufinden waren, wurde schon aus Support-Gründen eine Vereinheitlichung angestrebt und von der Abteilung Informations- und Kommunikationstechnik diesbezüglich das Projekt „Windows-XP-Migration“ initiiert. Seit Ende November 2004 findet ein flächendeckender Umstieg statt. Vor dem Umstieg habe ich mir die wesentlichen Unterschiede der Systeme erläutern lassen. Positiv im Sinne des Datenschutzes hervorzuheben ist, dass Windows XP SP2 ein differenzierteres Zugriffsrechte-System als die Vorgängersysteme bietet.

4. Remote-Control- Tool „Proxy“

Beim **rbb** soll in Kürze einheitlich das Remote-Control-Tool „Proxy“ eingesetzt werden. Am Standort Potsdam ist dieses Tool schon in der Vergangenheit unter dem Namen „CCM Remote Control“ im Einsatz gewesen. Mit dem Remote-Control-Tool können die Mitarbeiter des IT-Supports in die Lage versetzt werden, den Inhalt des Bildschirms einer Nutzerin/eines Nutzers auf dem eigenen Rechner angezeigt zu bekommen. Auf diese Weise kann in bestimmten Fällen auf den Vor-Ort-Support verzichtet werden. Da der Vorgang stets von der Rat suchenden Person initiiert und gesteuert wird, konnte ich nach meiner Vorabkontrolle das Tool aus datenschutzrechtlicher Sicht zur Nutzung freigeben.

5. Digitales Produktionssystem Fernsehen

Da im **rbb** Handlungsbedarf besteht, alte Schnittsysteme zu erneuern, wurde im Sommer 2004 das Projekt „Digitales Produktionssystem Fernsehen“ (DPS) initiiert. Dieses neue System soll zunächst ein vernetztes Arbeiten der Redaktionen „Abendschau“ und „Brandenburg aktuell“ an den unterschiedlichen Standorten so ermöglichen, dass z. B. gleiches Rohmaterial für unterschiedliche Beiträge genutzt werden kann, ohne dass Bandtransporte notwendig sind.

Weiterhin sollen die Produktionsabläufe durch dieses System verdichtet werden, damit der Redaktionsschluss ganz im Sinne der Aktualität näher an den Ausstrahlungszeitpunkt des Beitrages gelegt werden kann.

In einem ersten Informationsgespräch mit dem Projektleiter am 7. Januar 2005 habe ich darum gebeten, die anfallenden Nutzer- und Metadaten (bestimmte Angaben zu dem Beitrag wie Autor, Rechte, etc...) für meine datenschutzrechtliche Vorabkontrolle im Einzelnen aufzulisten. Dabei ist auch auf den Verarbeitungszweck und die Speicherdauer einzugehen. Ferner habe ich die Erarbeitung eines Berechtigungskonzeptes gefordert. Außerdem muss in einem Datensicherheitskonzept detailliert dargelegt werden, durch welche Maßnahmen die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz der Daten gewährleistet werden.

6. Neues Hörfunk-Dispositionssystem

In den Hörfunk-Programmen des **rbb** werden unterschiedliche Dispositionssysteme mit sehr verschiedenen Funktionen genutzt. Es soll nun ein neues System mit einheitlichen Eigenschaften hergestellt, angepasst und eingesetzt werden.

Dazu wurde ein Projektteam berufen, das aus den Disponenten der verschiedener Hörfunk-Bereiche (Technik und Programm), der Betreuerin des Hörfunk-Planungsprogramms und einem Projektleiter zusammengesetzt ist. In den bisherigen Teamsitzungen wurden zunächst die positiven Seiten und Schwächen der Arbeit mit den jetzigen Systemen und Verfahren analysiert und daraus Forderungen an ein neues System abgeleitet. Ich bin bereits in dieser frühen Phase mit einbezogen worden und hatte Gelegenheit, die von den Disponenten definierten Anforderungen um datenschutzrechtliche Anforderungen zu ergänzen.

II. Richtlinien

1. Richtlinien für die Nutzung von Lotus Notes und Richtlinien für die Nutzung von Internet und E-Mail

Zu den im Berichtszeitraum verabschiedeten „Richtlinien für die Nutzung von Lotus Notes“ und „Richtlinien für die Nutzung von Internet und E-Mail“ s. C I. 1.

2. Mobiltelefonrichtlinie

Derzeit ist eine neue Richtlinie für die Verwaltung und Nutzung mobiler Telekommunikationsgeräte in Arbeit. Darin sollen die Verwaltung der Geräte, die Bedingungen der Nutzung, die Abrechnung sowie die Rechnungsprüfung und -zuordnung geregelt werden. An der Erarbeitung dieser Richtlinie bin ich beteiligt.

3. Dienstanweisung für die Bearbeitung und Verwaltung von Dokumenten und Akten

Durch die Abteilung Organisation ist auf der Grundlage von § 35 Abs. 5 der Geschäftsordnung ein Entwurf für eine Dienstanweisung zum Umgang mit Dokumenten und Akten erarbeitet worden. Ziel der Dienstanweisung ist die rechtzeitige und wirtschaftliche Bereitstellung dokumentenbezogener Informationen und deren Vertraulichkeit, Integrität, Authentizität sowie Revisionsfähigkeit und Transparenz zu gewährleisten. Des Weiteren soll erreicht werden, die Kosten der Aufbewahrung auf ein Minimum zu beschränken.

An der Erarbeitung des Entwurfs war ich beteiligt. Die datenschutzrechtlichen Vorgaben sind berücksichtigt. Die Geschäftsleitung hat den Entwurf übernommen. Derzeit befindet er sich zur Information und Stellungnahme beim Personalrat.

4. Grundlegende, bislang nicht verabschiedete Richtlinien

Es ist im Berichtszeitraum leider nicht gelungen, die für Datenschutz und Datensicherheit im **rbb** grundlegenden Richtlinien zu verabschieden.

An erster Stelle zu nennen sind die Datenschutzrichtlinien. Sie sollen § 31 der **rbb**-Geschäftsordnung ergänzen und der praktischen Umsetzung der für den **rbb** geltenden datenschutzrechtlichen Bestimmungen dienen (§ 36 **rbb**-Staatsvertrag). In ihr sollen Rahmenregelungen für die automatisierte und nicht automatisierte Verarbeitung personenbezogener Daten enthalten sein.

Auf meinen den verantwortlichen Kolleginnen und Kollegen aus den IT-Bereichen vor einiger Zeit unterbreiteten Vorschlag habe ich bislang keine Resonanz erhalten. Das ist deshalb so bedauerlich, weil in den Datenschutz-Richtlinien grundlegende Regelungen getroffen werden sollen, auf die dann sämtliche spezielleren Regelungen aufbauen.

Darüber hinaus sollten jetzt dringend die PC- und die Wartungsrichtlinien verabschiedet werden, weil sie ebenfalls grundsätzliche organisatorische Fragen berühren.

III. Sonstiges

1. Stasi-Überprüfung im rbb

Der Rundfunkrat hat am 8. September 2003 empfohlen, eine Überprüfung der programmprägenden und leitenden fest angestellten sowie der programmprägenden freien Mitarbeiter/innen des **rbb** auf eine etwaige Zusammenarbeit mit dem Ministerium für Staatssicherheit der DDR zu veranlassen. Dieser Empfehlung ist die Intendantin gefolgt. An der Aufstellung des konkreten Verfahrens (Auskunftsersuchen, Umgang mit den Auskünften der Birtler-Behörde im Haus, etc...) war ich beteiligt. Inzwischen sind die Anträge bei der Birtler-Behörde gestellt. Ein Rücklauf ist noch nicht erfolgt.

2. Einführung des Online-Hotelbuchungssystems „hotel.de“

Mitte Dezember 2004 haben ARD und ZDF mit der hotel.de AG eine Großkundenrahmenvereinbarung mit dem Ziel abgeschlossen, den Rundfunkanstalten die Mög-

lichkeit zu geben, mit Hilfe eines Online-Buchungssystems Hotelreservierungen weltweit zu Großkundenkonditionen zu buchen.

Ich bin im Vorfeld in die Planungen mit einbezogen worden. Jetzt sind sämtliche Funktionen, die dazu geeignet sind, personenbezogene Auswertungen vorzunehmen, im System gesperrt. Damit ist sichergestellt, dass eine Leistungs- und Verhaltenskontrolle mit Hilfe dieses Systems nicht stattfinden kann.

3. Sonstiges

Die unterschiedlichsten Bereiche im **rbb** haben im Berichtszeitraum in Einzelfragen meinen Rat eingeholt. Dabei ging es z. B. um Fragen der Fachabteilungen zu Aufbewahrungspflichten von Akten, um die Umsetzung neuer rechtlicher Vorschriften durch die HA Personal und um die Modalitäten der Durchführung einer Umfrage zum Zwecke der Ermittlung des Bedarfs an Kinderbetreuung im **rbb** durch die Frauenvertreterin.

D. Datenschutz bei der Rundfunkteilnehmer-Datenverarbeitung

I. Allgemeines

Gemäß § 8 Abs. 2 Satz 1 Rundfunkgebührenstaatsvertrag (RGebStV) zieht die GEZ die Rundfunkgebühren für die Landesrundfunkanstalten ein und verarbeitet für diese als Auftraggeber die beim Gebühreneinzug anfallenden personenbezogenen Daten. Die Datenschutzkontrolle richtet sich nach dem für die jeweilige Anstalt geltenden Recht. Gemäß § 8 Abs. 2 Satz 2 RGebStV bestellt die GEZ eine/n betriebliche/n Datenschutzbeauftragte/n. Die/der Datenschutzbeauftragte der GEZ arbeitet eng mit den Rundfunkdatenschutzbeauftragten der einzelnen Häuser zusammen.

Die Datenschutzbeauftragten der Rundfunkanstalten haben die Bearbeitung und Beantwortung von Anfragen und sonstigem Routineschriftwechsel in Datenschutzangelegenheiten der Datenschutzbeauftragten der GEZ übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter und von individuellen

Anfragen mit besonderer datenschutzrechtlicher Bedeutung haben sie sich vorbehalten.

Die von der Datenschutzbeauftragten der GEZ, Frau Kerstin Arens, für den **rbb** beantworteten Anfragen lassen sich wie folgt kategorisieren:

- Ersuchen von Rundfunkteilnehmern um Auskunft über zu ihrer Person gespeicherten Daten: *insgesamt 2*
- Fragen bezüglich der Herkunft von Daten (z.B. Adressen) bzw. der Berechtigung zur Datenerhebung: *insgesamt 5*
- Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen: *insgesamt 3*
- Anfragen von Finanzämtern nach Daten (insbesondere Bankverbindungen) von Rundfunkteilnehmern: *insgesamt 65*
- Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von Rundfunkteilnehmern: *insgesamt 1*
- andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz: *insgesamt 5*

Die Anfragen der Finanzämter, die unter Bezug auf § 93 a AO um Auskunft über die bei der GEZ gespeicherten Bankverbindungen der Rundfunkteilnehmer zum Zwecke der Vollstreckung bei Steuerschulden ersuchten, wurden mit Hinweis auf den Grundsatz der Zweckbindung, der für die Verarbeitung der Rundfunkteilnehmerdaten gemäß § 3 Abs. 3 RGebstV gilt, - wie bisher - regelmäßig abschlägig beschieden. Das gleiche gilt für die Ersuchen der Kommunalkassen, ihnen bei der Aufenthaltsermittlung von Schuldnern öffentlich-rechtlicher Forderungen behilflich zu sein.

Es ist darauf hinzuweisen, dass die oben angegebene Menge der den **rbb** betreffenden Anfragen nicht sämtliche bei der GEZ eingegangenen Anfragen enthält. Solche Eingaben werden nicht vollständig der betrieblichen Datenschutzbeauftragten der GEZ zur Bearbeitung zugeleitet, sondern einfache Anfragen, z. B. nach der Herkunft

einer für ein Mailing verwendeten Adresse, bearbeitet aus Gründen der Zweckmäßigkeit und zur Beschleunigung der Abwicklung auch die Teilnehmerbetreuung der GEZ. - Die Datenschutzbeauftragte der GEZ hat mitgeteilt, dass sie insgesamt auf ihr Antwortschreiben im Jahr 2004 – wie auch im Vorjahr – so gut wie keine negativen Reaktionen erfahren hat. Es darf darauf geschlossen werden, dass sie die Maßnahmen der GEZ hinreichend erläutert hat und eventuelle Bedenken ausgeräumt werden konnten.

II. Projekt „ DV 2005“ bei der GEZ

Zentralen Raum aller Aktivitäten nahm bei der GEZ im Berichtszeitraum das Großprojekt „DV 2005“ (neues DV-System für den Rundfunkgebühreneinzug) ein. Der Produktivstart dieses neuen Systems soll zum 30. Mai 2005 erfolgen. Um sicherzustellen, dass die Rechte der Betroffenen gewahrt und die technischen und organisatorischen Maßnahmen ausreichend sind, wurde eine Arbeitsgruppe „Vorabkontrolle“ bei der GEZ eingerichtet. Diese Arbeitsgruppe hat sich unter dem Vorsitz der betrieblichen Datenschutzbeauftragte der GEZ u.a. mit folgenden Themen beschäftigt:

- Erstellung von Verfahrensverzeichnissen
- Aufbau der Datenbanken, d.h. Trennung der verschiedenen Datenbestände (Teilnehmer/potentielle Teilnehmer / sonstige Kontakte)
- Überprüfung der Datenmasken, des Benutzerhandbuchs sowie der Attributenliste zu DV 2005 unter datenschutzrechtlichen Gesichtspunkten
- Überprüfung des sog. Personenkonzeptes und damit zusammenhängender Detailfragen
- Zugriffsregelung auf LRA-fremde Teilnehmerkonten
- Löschung bzw. Sperrung von Daten
- Anonymisierung von Test- und Schulungsdaten
- Fragen des Berechtigungskonzeptes/User Access Management
- Verfolgung von Change Requests mit datenschutzrechtlichem Bezug.

Im Einvernehmen mit den jeweiligen Fachbereichen bzw. den Projektverantwortlichen wurde festgelegt, dass diverse ursprünglich vorgesehene Attribute bzw. Kennzeichen mangels entsprechender Rechtsgrundlage nicht im neuen System gespeichert werden.

Am 17. Mai 2004 haben sich die Rundfunkdatenschutzbeauftragten über den Stand des Projekts bei der GEZ informiert und ihre Vorstellungen einbringen können. Dabei haben wir uns insbesondere mit Fragen des Aufbaus der Datenbanken bzw. der Trennung der verschiedenen Datenbestände beschäftigt und Einzelfragen aus der Attributenliste erörtert. Eine weitere Befassung der Rundfunkdatenschutzbeauftragten mit „DV 2005“ erfolgte auf einem Treffen am 1. September 2004 bei der GEZ, das der Vorbereitung der seinerzeit bevorstehenden Prüfung der GEZ durch die Landesdatenschutzbeauftragten von Bremen, Hessen, Brandenburg und Berlin diente (s. dazu III.). Ungefähr einen Monat nach Produktivstart des Systems werden wir bei der GEZ überprüfen, ob sämtliche datenschutzrechtlichen Anforderungen auch tatsächlich im System berücksichtigt worden sind.

III. Prüfung der GEZ durch die Landesdatenschutzbeauftragten von Bremen, Hessen, Berlin und Brandenburg

Im September 2004 haben die Landesdatenschutzbeauftragten von Hessen, Bremen, Brandenburg und Berlin eine gemeinsame datenschutzrechtliche Kontrolle der GEZ durchgeführt. An der dreitägigen Prüfung haben neben den Vertretern der genannten Landesdatenschutzbeauftragten auch einige Rundfunkdatenschutzbeauftragte und andere Mitarbeiter der von der Prüfung betroffenen Rundfunkanstalten teilgenommen. Schwerpunkte der Prüfung waren die Organisation der Datensicherheit, der Umfang der Datenverarbeitung im aktiven Teilnehmerkonto, die Verarbeitung von Meldedaten, die Verarbeitung von Adressdaten aus dem privaten Adresshandel, das Lösungskonzept der GEZ, die Datenverarbeitung im Rahmen der Gebührenbefreiung, die Datenverarbeitung durch die Gebührenbeauftragten und die Datenverarbeitung durch externe Dienstleister im Auftrag der GEZ. Kontroverse Diskussionen entstanden erwartungsgemäß vor allem zu den Themen Mailing und der Auslagerung diverser Arbeiten an externe Firmen. Der endgültige Prüfbericht liegt noch nicht vor.

IV. Schulung der Rundfunkgebührenbeauftragten

Am 30. November und am 14. Dezember 2004 habe ich jeweils zusammen mit dem Systemverantwortlichen IT-Sicherheit, Herrn Gerry Wolff aus der Abteilung Informations- und Kommunikationstechnik, eine zweistündige Datenschutzbildung für die Rundfunkgebührenbeauftragten von Berlin und Brandenburg durchgeführt. Dabei habe ich die datenschutzrechtlichen Rahmenbedingungen für die Rundfunkteilnehmerdatenverarbeitung dargestellt. Außerdem bin ich auf die zum Zwecke der Datensicherheit zu ergreifenden organisatorischen Maßnahmen eingegangen. Herr Wolff richtete sich mit seinen technischen Ausführungen an diejenigen Rundfunkgebührenbeauftragten, die bei ihrer Arbeit für den **rbb** auch einen PC oder Laptop verwenden. In der anschließenden Diskussion, an der sich die Teilnehmerinnen und Teilnehmer lebhaft beteiligten, ging es hauptsächlich darum, für datenschutzrelevante Probleme, die bei der täglichen Arbeit der Rundfunkgebührenbeauftragten immer wieder auftreten, Lösungen zu finden.

Herr Wolff und ich beabsichtigen, auch in Zukunft weiterhin regelmäßige Schulungen für die Rundfunkgebührenbeauftragten anzubieten. Außerdem haben wir uns vorgenommen, in Kürze stichprobenartig datenschutzrechtliche Prüfungen bei einzelnen Rundfunkgebührenbeauftragten vor Ort durchzuführen.

E. Datenschutz im Informationsverarbeitungszentrum (IVZ)

I. Allgemeines

MDR, **rbb**, Radio Bremen, NDR, SR und DLR (die vier letztgenannten als Teilkoooperationspartner) betreiben als gemeinschaftliche Einrichtung das Informations-Verarbeitungs-Zentrum (IVZ) im Rahmen einer öffentlich-rechtlichen nicht-rechtsfähigen Verwaltungsgemeinschaft mit Sitz beim **rbb**.

Gegenstand ist u. a. die Erfassung, Verarbeitung und Nutzung von Daten, einschließlich der Verarbeitung und Nutzung von Daten zu eigenen journalistisch-redaktionellen Zwecken der Rundfunkanstalten, der Einrichtung von Datenbanken,

der Programmerstellung und Software-Entwicklung sowie der Durchführung von Arbeiten im Bereich betriebswirtschaftlicher und archivarischer EDV-Anwendungen für die Rundfunkanstalten.

Für die Datenschutzkontrolle beim IVZ sind alle Rundfunkdatenschutzbeauftragten der beteiligten Rundfunkanstalten zuständig. Wie üblich bei ARD-Gemeinschaftseinrichtungen wurde die Federführung für die Datenschutzkontrolle vor Ort mir als der Datenschutzbeauftragten der Sitzanstalt übertragen.

In Grundsatzangelegenheiten beziehe ich die Kolleginnen und Kollegen der anderen Rundfunkanstalten ein. Außerdem finden regelmäßig Zusammenkünfte aller beteiligten Rundfunkdatenschutzbeauftragten beim IVZ statt.

Angesichts der Größe des Rechenzentrums haben die Datenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten im Herbst 2004 - unabhängig von der Rechtslage, die eine Bestellung nicht zwingend vorschreibt - dafür plädiert, wie bei der GEZ in Köln auch im IVZ einen eigenen betrieblichen Datenschutzbeauftragten zu bestellen. Dieser Datenschutzbeauftragte soll für die Rundfunkdatenschutzbeauftragten als Ansprechpartner fungieren.

Mit Wirkung zum 1. Oktober 2004 hat der Geschäftsführer des IVZ, Herr Dr. Greten, den Mitarbeiter aus der R/3-Basisbetreuung Herrn Lutz Schade nebenamtlich zum betrieblichen Datenschutzbeauftragten des IVZ bestellt.

II. Einzelne Themen

Auf dem Treffen der Datenschutzbeauftragten der das IVZ betreibenden Rundfunkanstalten mit der Geschäftsleitung des IVZ am 7. Mai 2004 wurden insbesondere das Risikomanagement, die Backupstrategie, die Netzwerksicherheit und die Hardwarestrategie SAP beim IVZ erörtert.

Inzwischen dient das IVZ mit unterschiedlichen Anwendungen fast allen Landesrundfunkanstalten als Rechenzentrum. Aus diesem Grund war das Treffen der Da-

tenschutzbeauftragten der betreibenden Anstalten am 13. Oktober 2004 beim IVZ auch für die Datenschutzbeauftragten der als Auftraggeber mit dem IVZ verbundenen Anstalten offen. Im Anschluss an eine Präsentation der Tätigkeitsfelder des IVZ, ging es im Schwerpunkt um die Archiv-Projekte für die einzelnen Rundfunkanstalten.

Auf der Sitzung hat sich auch der neue betriebliche Datenschutzbeauftragte des IVZ vorgestellt. Von Seiten der Datenschutzbeauftragten wurde problematisiert, dass Herr Schade im Hauptamt im operativen Bereich beim IVZ beschäftigt ist, wodurch Interessenkonflikte nicht auszuschließen sind.

Herr Schade wurde damit beauftragt, bis zum nächsten Zusammentreffen der Datenschutzbeauftragten beim IVZ Ende Mai 2005 den Datenschutzbeauftragten der Betreiberanstalten eine Zusammenstellung aller Wartungsverträge, die das IVZ mit Externen abgeschlossen hat, ergänzt um eine Bewertung hinsichtlich der Einhaltung der einschlägigen datenschutzrechtlichen Bestimmungen zukommen zu lassen. Ferner wurde er gebeten, die „Datenschutz-/Datensicherungsmaßnahmen und Arbeitsrichtlinien im IVZ mit Stand 3. Mai 2000“ fortzuschreiben.

F. Datenschutz im ARD-Hauptstadtstudio (HSB)

Das allgemein wachsende Bedürfnis nach „Mobility“ spielt auch im HSB eine immer größere Rolle. Der Wunsch, jederzeit - auch von außen - auf die sog. PIM (Personal Information Management)- Daten zugreifen zu können, ist insbesondere bei den Journalistinnen und Journalisten stark ausgeprägt. Zu den PIM-Daten gehören die persönlichen E-Mails, Kontakte, Termine, etc. Bei der Entwicklung gesicherter Zugriffsmethoden wurde ich von dem Verantwortlichen für Hörfunk- und IT-Systeme beim ARD-HSB, Herrn Wolfgang Zülch, mit einbezogen.

G. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR (AK DSB) ist im Berichtszeitraum unter dem Vorsitz des Datenschutzbeauftragten des SWR, Herrn Prof. Herb, drei Mal zusammengekommen. Bis Ende 2005 bin ich zur stellvertretenden Vorsitzenden des AK DSB gewählt. Am 22./23. April 2004 fand eine Sitzung beim SWR in Friedrichshafen statt. Der Arbeitskreis beschäftigte sich vor allem mit Fragen aus dem Bereich des Rundfunkteilnehmerdatenschutzes, speziell mit dem Projekt DV 2005 der GEZ, dem Abmeldeverfahren und dem „direct mailing“ und bereitete die Prüfung der GEZ durch die Landesdatenschutzbeauftragten von Hessen, Bremen, Brandenburg und Berlin vor. Auf der Sitzung am 30.9./1.10.04 in Bonn wurde u. a. intensiv über die Frage des Verhältnisses von Datenschutz auf der einen und Informantenschutz und Redaktionsgeheimnis auf der anderen Seite sowie über Datenschutz in den Fernseh- und Hörfunkarchiven diskutiert. Auf der Sitzung am 10./11. März 2005 in Saarbrücken hat der Arbeitskreis sich erneut im Schwerpunkt mit dem Rundfunkteilnehmerdatenschutz beschäftigt. Dabei ging es im wesentlichen um den Stand der datenschutzrechtlichen Prüfung des Projektes „DV 2005“, die mit dem Inkrafttreten des 8. Rundfunkänderungsstaatsvertrages zum 1. April 2005 eintretenden Änderungen im Verfahren bei der Befreiung von der Rundfunkgebühr, die Auslegung des neuen § 8 Abs. 4 Rundfunkgebühren-Staatsvertrag und die Neufassung der Richtlinien für den Datenschutz der GEZ.

Der Datenschutzbeauftragte des Norddeutschen Rundfunks, Herrn Maximilian Meriten, vertritt den AK DSB in der Arbeitsgruppe nach Art. 29 EU-Datenschutzrichtlinie, der alle Datenschutzkontrollstellen der Mitglieder der Europäischen Union angehören.

II. IT-Sicherheitsgremium für das ARD-Corporate Network

Die ARD betreibt mit dem ARD-Daten-Corporate Network (ARD-CN) einen Datenverbund zwischen den Landesrundfunkanstalten. Das ARD-CN gewinnt für den Informationsaustausch zwischen den Rundfunkanstalten, gerade auch für den Sendebetrieb, immer mehr an Bedeutung. Durch die Verknüpfung der Kommunikationswege der Rundfunkanstalten erhöht sich das Risiko des Verlustes der Vertraulichkeit, Verfügbarkeit und Integrität der ausgetauschten Informationen und der Sicherheit der Informationssysteme in den einzelnen Rundfunkanstalten.

Im Herbst 2003 wurde eine interdisziplinäre Arbeitsgruppe damit beauftragt worden, eine Erhebung zur IT-Sicherheit in den einzelnen Häusern durchzuführen und Sicherheitsrichtlinien für das ARD-CN zu erarbeiten. Ich habe dieser Arbeitsgruppe als Vertreterin des AK DSB angehört.

Die Erhebung hat ergeben, dass in den einzelnen ARD-Anstalten die Relevanz des Themas IT-Sicherheit bislang sehr unterschiedlich bewertet worden ist. Die Arbeitsgruppe hat eine Vereinbarung zur informationstechnischen Sicherheit im ARD-CN erarbeitet, die die Grundlage für die Arbeit eines IT-Sicherheitsgremiums bildet. Diese Vereinbarung ist zusammen mit konkreten Empfehlungen u. a. zum Virenschutz und zur Systemsicherheit bei Nutzung des ARD-CN inzwischen und zu Anforderungen an Dienste, Anwendungen bzw. Applikationen im ARD-CN von der Produktions- und Technik -Kommission (PTKO) und Finanzkommission (FIKO) verabschiedet worden. Mit der Verabschiedung dieser Papiere endete die Arbeit dieser interdisziplinären Arbeitsgruppe.

Wie in der Vereinbarung vorgesehen, wurde allerdings inzwischen das IT-Sicherheitsgremium gebildet. Jede ARD-Anstalt hat eine/n sog. IT-Sicherheitsbeauftragte/n in dieses Gremium entsandt. Der **rbb** wird durch den Systemverantwortlichen IT-Sicherheit, Herrn Gerry Wolff vertreten. Außerdem gehören als beratende Mitglieder dem IT-Sicherheitgremium noch ein Vertreter des ARD-Sternpunktes und je ein/e Vertreter/in der ebenfalls an das CN angeschlossenen

Rundfunkanstalten ZDF, SRG, ORF sowie je ein/e Vertreter/ in der Arbeitskreise AK DSB, AG Informatik und TKTN (= Telekommunikation Kommunikationstechnik und Netze) an. Ich vertrete den AK DSB in diesem Gremium, das ansonsten ausschließlich aus Technikern und Technikerinnen besteht. Am 23. März 2005 hat die konstituierende Sitzung beim MDR in Leipzig stattgefunden. Zum Vorsitzenden des IT-Sicherheitsgremiums wurde der IT-Sicherheitsbeauftragte des WDR, Herr Gust gewählt. Sein Stellvertreter ist Herr Dr. Höhne vom NDR.

III. Teilnahme an Veranstaltungen

Am 2. April 2004 nahm ich an einer Veranstaltung des Instituts für Urheber- und Medienrecht in München zum Thema „Medienfreiheit und Datenschutz“ teil. Dabei ging es um die derzeitige Struktur der Datenschutzkontrollstellen in der Bundesrepublik Deutschland im allgemeinen, um die Funktion der Rundfunkdatenschutzbeauftragten sowie um das Verhältnis des grundgesetzlich verankerten Rechts der Medienfreiheit zum Grundrecht auf Datenschutz.

Am 13./14. Mai 2004 nahm ich an einer Tagung der Alcatel SEL Stiftung für Kommunikationsforschung in Stuttgart zum Thema „Neuordnung des Medienrechts – neuer rechtlicher Rahmen für eine konvergente Technik?“ teil. Diskutiert wurde unter anderem darüber, welchen Ordnungsrahmen die Fortentwicklung der Medien braucht. Die Neuregelung des Datenschutzes in den elektronischen Medien bildete einen Schwerpunkt der Veranstaltung.

Berlin, 28. April 2005

gez. Anke Naujock