

3. Tätigkeitsbericht

der Beauftragten für den Datenschutz
des Rundfunk Berlin-Brandenburg

Berichtszeitraum:

1. April 2005 bis 31. März 2006

Dem Rundfunkrat gemäß § 38 Abs. 7 **rbb**-Staatsvertrag

vorgelegt von Anke Naujock

Vorbemerkung

Auch im Berichtsjahr ließen sich meine Aufgaben wieder in folgende fachliche Bereiche gliedern:

- ? Mitarbeit an **rbb**-internen Regelungen mit datenschutzrechtlicher Relevanz,
- ? datenschutzrechtliche Überprüfung, Begleitung und Vorabkontrolle von Projekten und Regelungen,
- ? Bearbeitung von Anfragen und Beschwerden und
- ? Informations- und Öffentlichkeitsarbeit.

Den Schwerpunkt bildete der Datenschutz beim Rundfunkgebühreneinzug. Dabei war die Bandbreite der Fragestellungen weit gefächert:

Zusammen mit den anderen Rundfunkdatenschutzbeauftragten habe ich mich ausführlich mit den Kritikpunkten im gemeinsamen Bericht der Landesdatenschutzbeauftragten von Bremen, Hessen, Berlin und Brandenburg vom 1. Juni 2005 über die Prüfung der GEZ vom 21. bis 23. September 2004 auseinandergesetzt (D II).

Seit Herbst 2005 beschäftige ich mich zusammen mit den anderen Rundfunkdatenschutzbeauftragten mit den Plänen der GEZ zum Aufbau einer sog. NP (NichtPrivate)-Datenbank zur besseren und systematischen Ausschöpfung des nichtprivaten Marktes (D V).

Die Auswirkungen des 8. Rundfunkänderungsstaatsvertrages waren ein weiteres zentrales Thema. Hierbei ging es insbesondere darum, im Zusammenwirken mit der GEZ, den anderen Rundfunkdatenschutzbeauftragten und den Landesdatenschutzbeauftragten eine datenschutzgerechte Lösung für die Umsetzung des neuen § 6 Abs. 2 Rundfunkgebührenstaatsvertrag (RGebStV) zu erreichen (B III 1.1).

Die ersten Monate des Jahres 2006 standen ganz unter der Überschrift: Aktualisierung der technischen und organisatorischen Maßnahmen zum Datenschutz in der Rundfunkgebührenstelle und bei den für den **rbb** tätigen Rundfunkgebührenbeauftragten (D IX).

Daneben galt es, die Themen Datenschutz und Datensicherheit auch in den übrigen Bereichen des **rbb** weiter voranzutreiben.

Am 21. November 2005 trat endlich die Datenschutz-Dienstanweisung, der Grundstein für alle weiteren datenschutzrechtlichen Regelungen im **rbb**, in Kraft. Das dort geregelte Verfahren bei der Vorabprüfung neuer Systeme, mit denen personenbezogene Daten verarbeitet werden, konnte bereits bei zahlreichen Projekten des **rbb** mit Erfolg angewandt werden.

Bedanken möchte ich mich auch in diesem Jahr bei der Intendantin, den weiteren Mitgliedern der Geschäftsleitung und den sonstigen Verantwortungsträgern für das mir entgegengebrachte Vertrauen. Meinen Empfehlungen wurde auch im Berichtszeitraum wieder ausnahmslos gefolgt.

Dem Systemverantwortlichen IT-Sicherheit, Herrn Gerry Wolff, danke ich für die konstruktive Zusammenarbeit und Unterstützung. Mit dem Personalrat konnte ich auch im Berichtszeitraum wieder einige gemeinsame datenschutzrechtliche Ziele erreichen. Auch ihm sei gedankt.

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

I. Gesetzliche Grundlagen

Die Rechtsgrundlagen für die Tätigkeit der Datenschutzbeauftragten des **rbb** haben sich im Berichtszeitraum nicht verändert.

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

Gemäß Abs. 2 Satz 2 überwacht er/sie die Einhaltung der Datenschutzvorschriften des **rbb**-Staatsvertrags und anderer Vorschriften über den Datenschutz, soweit der **rbb** personenbezogene Daten zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet.

Soweit eine Befugnis des oder der Beauftragten für den Datenschutz nach Abs. 2 Satz 1 nicht gegeben ist, obliegt die Kontrolle der Einhaltung von Datenschutzbestimmungen beim **rbb** dem oder der Landesbeauftragten für den Datenschutz des Landes Berlin. Die Kontrolle erfolgt im Benehmen mit dem oder der Landesbeauftragten des Datenschutzes des anderen Landes (Abs. 8).

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

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

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 **rbb** bestellt.

Parallel dazu hat mich die Intendantin für den gleichen Zeitraum mit der Wahrnehmung der Aufgaben der behördlichen Datenschutzbeauftragten im Sinne von § 19a BlnDSG beauftragt. Eine Stellvertretung für die behördliche Datenschutzbeauftragte ist nach wie vor nicht bestellt. Meine Funktion als Datenschutzbeauftragte des **rbb** nehme ich nebenamtlich zu meiner Tätigkeit im Justitiariat wahr.

Am 19. Mai 2005 hat der Brandenburgische Landtag Frau Dagmar Hardtke zur neuen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg gewählt. Frau Hardtke war bislang stellvertretende Berliner Datenschutzbeauftragte.

Am 2. Juni 2005 wurde der ehemalige Landesbeauftragte für den Datenschutz und das Rechts auf Akteneinsicht in Brandenburg, Herr Dr. Alexander Dix, vom Berliner Abgeordnetenhaus zum Berliner Beauftragten für Datenschutz und Informationsfreiheit gewählt.

Die Zusammenarbeit mit beiden Stellen, die sich auf den Datenschutz bei Rundfunkgebühreneinzug beschränkt hat, war im Berichtszeitraum im Wesentlichen konstruktiv und reibungslos. In vielen Fragestellungen gab es erfreuliche inhaltliche Übereinstimmungen in der datenschutzrechtlichen Bewertung.

Diese positiven praktischen Erfahrungen ändern freilich nichts an meinem Rechtsstandpunkt, wonach die Aufspaltung der Kontrollkompetenzen, die es vergleichbar außer beim **rbb** nur noch beim Hessischen Rundfunk und bei Radio Bremen gibt, verfassungsrechtlich zumindest bedenklich ist.

B. Entwicklung des Datenschutzrechts

I. Europa

1. Gesetzgebung

1.1 Die Europäische Verfassung

Der am 29. Oktober 2004 von den Staats- und Regierungschefs unterzeichnete Vertrag über eine Verfassung für Europa, den diese am 18. Juni 2004 einstimmig angenommen hatten, hätte nach der Ratifizierung durch alle Mitgliedstaaten ab dem 1. November 2006 in Kraft treten können. Damit wäre auch die darin erfolgte doppelte Verankerung des Rechts auf informationelle Selbstbestimmung (Art. I-51 und II-8) wirksam geworden.

In der Bundesrepublik erfolgte die Ratifizierung des EU-Verfassungsvertrages am 12. Mai 2005 durch den Bundestag und am 27. Mai 2005 durch den Bundesrat jeweils mit klarer Mehrheit. Mit dem Scheitern der Referenden in Frankreich und in den Niederlanden ist ein zeitnahes Inkrafttreten der EU-Verfassung nun ausgeschlossen.

1.2 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Kommunikationsdaten

In der Europäischen Datenschutzrichtlinie ist – wie in den deutschen Datenschutzgesetzen – der allgemeine datenschutzrechtliche Grundsatz verankert, wonach personenbezogene Daten zu löschen sind, sobald sie nicht mehr benötigt werden. Für die Kommunikationsdaten ist das grundsätzlich dann der Fall, wenn sie zur Übermittlung einer Nachricht bzw. zur Abrechnung nicht mehr benötigt werden. Gemäß Artikel 15 der Europäischen Datenschutzrichtlinie sind von diesem Grundsatz Ausnahmen zu Zwecken der Aufrechterhaltung der öffentlichen Ordnung, d. h. für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen zulässig.

Einige Mitgliedstaaten – Deutschland gehört nicht dazu – haben bereits Rechtsvorschriften über eine verdachtsunabhängige Vorratsspeicherung von Daten durch Diensteanbieter zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erlassen. Diese nationalen Vorschriften weichen stark voneinander ab.

Mit der Richtlinie 2006/24/EG haben das Europäische Parlament und der Rat der Europäischen Union nun zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten eine Pflicht zur verdachtsunabhängigen Vorratsspeicherung von Verbindungsdaten statuiert. Die Mitgliedstaaten haben sich verpflichtet, den Telekommunikationsanbietern eine Speicherfrist von mindestens sechs Monaten für die Verbindungsdaten aufzuerlegen. Es steht ihnen frei, die Frist im nationalen Recht bis auf 24 Monaten anzuheben. Inhalte werden nicht erfasst.

Die Richtlinie muss bis spätestens 15. September 2007 von den Mitgliedstaaten umgesetzt werden. Bis zum 15. März 2009 kann jeder Mitgliedstaat die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail aufschieben. Deutschland hat erklärt, von dieser Möglichkeit des Aufschiebs Gebrauch zu machen.

Die Datenschutzbeauftragten in Europa und Deutschland haben dieses Vorhaben bis zuletzt grundsätzlich abgelehnt, weil dadurch das in der Europäischen Menschenrechtskonvention garantierte Recht auf freie und unbeobachtete Kommunikation verletzt wird. Vor allem der Quellen- und Informantenschutz ist in Gefahr. Zwar gibt es eine Klausel, der zufolge das Berufsgeheimnis bei bestimmten Gruppen gewahrt werden könne, doch ist dies nur eine vage Formulierung.

Es wird nun darum gehen, dass der deutsche Gesetzgeber die verbleibenden Spielräume der europäischen Rahmenregelung etwa hinsichtlich des Speicherungszeitraumes und der Verwendungszwecke der gespeicherten Verkehrsdaten so restriktiv und so Grundrechts schonend wie möglich nutzt und überdies dem Quellen- und Informantenschutz Rechnung trägt.

2. Sonstiges

- Einleitung eines Vertragsverletzungsverfahrens

Im Juli 2005 leitete die Europäische Kommission ein Vertragsverletzungsverfahren gegen die Bundesrepublik ein, weil sie die Auffassung vertritt, dass die Stellung der Aufsichtsbehörden für den nicht-öffentlichen Bereich in allen 16 Ländern der Bundesrepublik Deutschland gegen Art. 28 der Datenschutzrichtlinie 95/46/EG verstößt. Darin wird eine „völlige Unabhängigkeit“ dieser Aufsichtsbehörden europaweit vorgeschrieben. Die Bundesregierung hat in ihrer Stellungnahme gegenüber der Kommission ihren alten Standpunkt bekräftigt, wonach das System der Datenschutzkontrolle gerade im nicht-öffentlichen Bereich durch die Datenschutzrichtlinie nicht verändert werden sollte. Es ist davon auszugehen, dass die Europäische Kommission den Europäischen Gerichtshof anrufen wird, dessen Entscheidung weitreichende Konsequenzen für die Struktur der Datenschutzaufsicht in Deutschland haben könnte.

II. Deutschland

1. Gesetzgebung

1.1 Strafprozessordnung (StPO)

Mit seinem Urteil vom 3. März 2004 (Az.: 1 B VR 2378/98, 1 B 1084/99) hatte das Bundesverfassungsgericht bekanntlich festgestellt, dass die einschlägigen Vorschriften der Strafprozessordnung (StPO) zur akustischen Wohnraumüberwachung den Vorgaben des Artikel 13 Abs. 3 GG nicht hinreichend Rechnung trugen. Es hatte dem Gesetzgeber aufgegeben, einen verfassungsgemäßen Zustand bis spätestens 30. Juni 2005 herzustellen.

Mit Wirkung zum 1. Juli 2005 ist das „Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung)“ in Kraft getreten.

Entsprechend den vom Bundesverfassungsgericht aufgestellten Anforderungen ändert das Gesetz vor allem die Regelungen der Strafprozessordnung. So darf die akustische Wohnraumüberwachung nur beim Vorliegen des Verdachts einer besonders schweren Straftat aus dem in § 100c Abs. 2 StPO aufgeführten Katalog angeordnet werden.

Wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem privaten Kernbereich zuzuordnen sind, erfasst werden, ist die Überwachung zu unterbrechen und die Aufzeichnungen darüber sind zu löschen (§ 100 c Abs. 5).

Das Abhören von Berufsgeheimnisträgern – dazu zählen auch die Journalisten - ist unzulässig (§ 100 c Abs. 6).

1.2 Bundes-Informationsfreiheitsgesetz

Nach langen Beratungen und politischen Kontroversen ist am 1. Januar 2006 das Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz – IFG) in Kraft getreten. Damit erhält jeder – unabhängig von einer persönlichen Betroffenheit - ein Recht auf freien Zugang zu amtlichen Informationen der öffentlichen Stellen des Bundes. Der Anspruch auf Informationszugang umfasst alle Aufzeichnungen, die amtlichen Zwecken dienen, also sowohl Schriftstücke als auch Daten, die in Computersystemen gespeichert sind. In einer Reihe von Ausnahmefällen darf der Informationszugang allerdings ganz oder teilweise verweigert werden, etwa zum Schutz besonderer öffentlicher Belange (z. B. der inneren und äußeren Sicherheit oder der Durchführung von Gerichts- und Ermittlungsverfahren), personenbezogener Daten, des geistigen Eigentums oder von Betriebs- und Geschäftsgeheimnissen. Werden die gewünschten Informationen verwehrt, muss die öffentliche Stelle dies begründen. Gegen ablehnende Entscheidungen sind Widerspruch und Klage möglich. Jeder, der sein Recht auf Informationszugang beeinträchtigt sieht, kann sich an den Bundesdatenschutzbeauftragten wenden, der auch

der sog. Bundesbeauftragte für die Informationsfreiheit ist. Insoweit erfolgte auch eine Anpassung des Bundesdatenschutzgesetzes.

Das Informationsfreiheitsgesetz kann unter Umständen bei der verdeckten Recherche nützlich sein. Anders als bei den presserechtlichen Auskunftsansprüchen muss zur Geltendmachung des Anspruchs kein besonderes Interesse von den Journalisten dargelegt werden.

In den Ländern Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein gibt es schon seit einigen Jahren entsprechende Gesetze. Das Brandenburgische Akteneinsichts- und Informationszugangsgesetz (AIG) datiert vom 10. März 1998, das Gesetz zur Förderung der Informationsfreiheit im Land Berlin vom 15. Oktober 1999. Während das Brandenburgische Gesetz keine Auskunftsansprüche gegenüber dem **rbb** einräumt, ist die Rechtslage nach dem Berliner Gesetz in diesem Punkt zumindest zweifelhaft. Jedenfalls für den journalistisch-redaktionellen Bereich muss die Anwendbarkeit schon wegen Art. 5 Abs. 1 Satz 2 GG (Rundfunkfreiheit) ausscheiden.

1.3 Telemediengesetz – TMG/9. Rundfunkänderungsstaatsvertrag

Seit Mai 2005 liegen Entwürfe für ein Telemediengesetz des Bundes und einen Rundfunkänderungsstaatsvertrag der Länder vor. Hierzu führten der Bund und die Länder eine gemeinsame Anhörung der kommunalen Spitzenverbände, Fachkreise und Verbände durch. Bei der Anhörung waren auch die Rundfunkdatenschutzbeauftragten vertreten.

Die Gesetzgebungsinitiative hat zum Ziel, die bisher bestehenden unterschiedlichen Rechtsvorschriften für Informations- und Kommunikationsdienste bei weitgehender Beibehaltung des materiellen Rechts zusammenzufassen. Die geltenden Vorschriften des Teledienstgesetzes (TDG), des Teledienstedatenschutzgesetzes (TDDSG) und des Mediendienste-Staatsvertrages sollen durch ein einheitliches Telemediengesetz (TMG) des Bundes weitgehend ersetzt werden. Soweit bei journalistisch - redaktionell gestalteten Diensten eine Gesetzgebungskompetenz der Länder besteht, sollen die dafür erforderlichen spezifischen Vorschriften im Rundfunkstaats-

vertrag geregelt werden. Hinsichtlich der Datenschutzbestimmungen sind dabei umfassende dynamische Verweisungen auf das Telemediengesetz vorgesehen.

1.4 Konsequenz aus der „Cicero“-Affäre – Gesetzentwürfe der Grünen und der FDP zur Stärkung der Presse- und Rundfunkfreiheit

Die Bundestagsfraktionen der Grünen und der FDP haben jeweils Gesetzesentwürfe verabschiedet, mit denen die Presse- und Rundfunkfreiheit gestärkt werden soll. Es geht darum, eine notwendige Klarstellung zu erreichen, dass Medienangehörige sich nicht wegen Teilnahme am Geheimnisverrat dadurch strafbar machen, dass sie das ihnen zugespielte Material veröffentlichen. Hausdurchsuchungen in Wohnungen von Journalisten sollen zudem nur noch von einem Richter angeordnet werden können. Zugleich sollen die Journalisten bei Auskunftsbeglehen nach Verbindungs- und Standortdaten aus dem Telekommunikationsbereich durch Sicherheitsbehörden genauso geschützt werden, wie andere so genannte Berufsheimnisträger, also etwa Ärzte, Anwälte oder Priester.

Auslöser dieser Initiative war die sog. Cicero-Affäre, in deren Verlauf im vergangenen Herbst Staatsanwaltschaft und Polizei nach der Veröffentlichung eines Berichts über den jordanischen Terroristenführer Abu Musab al-Sarkawi mit Hinweis auf vertrauliches Material des Bundeskriminalamtes Durchsuchungen der Redaktion des Polit-Magazins Cicero sowie beim Autor des Artikels durchführten. Die Grünen und die FDP sehen durch das Handeln der Staatsmacht Meinungs- und Pressefreiheit gefährdet. Sie wollen verhindern, dass Strafverfolgungsbehörden den Informantenschutz unterlaufen und die Pflicht der Journalisten zur Information der Öffentlichkeit unter mannigfachen Strafverdacht gestellt wird.

Die von den Grünen und der FDP geforderten Gesetzesänderungen sind unbedingt erforderlich. Ihre Initiative sollte daher unterstützt werden.

2. Rechtsprechung

2.1 Bundesverfassungsgerichtsurteil vom 27. Juli 2005 (1 BvR 668/04) zur vorbeugenden Telefonüberwachung

Im Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung waren der Polizei in § 33 a Abs. 1 Nr. 2 und 3 Befugnisse zur Telekommunikationsüberwachung zum Zwecke der Verhütung und der Vorsorge für die Verfolgung von Straftaten eingeräumt worden.

Auf die Verfassungsbeschwerde eines Richters hat das Bundesverfassungsgericht mit Urteil vom 27. Juli 2005 festgestellt, dass die Regelungen wegen Verstoßes gegen das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG nichtig sind.

Teilweise habe der niedersächsische Gesetzgeber seine Gesetzgebungskompetenz überschritten. Denn der Bundesgesetzgeber habe die Verfolgung von Straftaten durch Maßnahmen der Telekommunikationsüberwachung in der Strafprozessordnung abschließend geregelt, so dass die Länder insoweit von der Gesetzgebung ausgeschlossen seien.

Auch materiell hat das Bundesverfassungsgericht die Befugnis zur präventiven Telekommunikationsüberwachung im Niedersächsischen Landesrecht für verfassungswidrig erklärt. Es hat seine Forderung bekräftigt, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben müssen.

2.2 Bundesverfassungsgerichtsurteil vom 2. März 2006 (2 BvR 2099/04) über die Bedingungen für die Beschlagnahme von Handy- und E-Mail-Verbindungsdaten

Mit Urteil vom 2. März 2006 (2 BvR 2099/04) hat das Bundesverfassungsgericht die Bedingungen für die Beschlagnahme von Handy- und E-Mail-Verbindungsdaten

erleichtert, die auf dem jeweiligen Gerät des Empfängers gespeichert sind. Nach dem Urteil unterliegen die Verbindungsdaten nicht mehr dem Fernmeldegeheimnis, sobald sie beim Empfänger eingegangen sind und der Übertragungsvorgang beendet ist. Die Beschlagnahme der Daten bei einer Durchsuchungsaktion müsse allerdings „verhältnismäßig“ sein und das Recht auf informationelle Selbstbestimmung wahren. Letztlich erleichtert das Urteil den Fahndern den Zugriff auf Handy- und Computerdaten, die nun nur noch durch das Recht auf informationelle Selbstbestimmung geschützt sind. Damit reicht den Fahndern schon ein Verdacht auf leichtere Straftaten, um die Beschlagnahme entsprechender Daten zu veranlassen. Das Fernmeldegeheimnis sanktioniert solche Zugriffe nur bei einem Verdacht auf schwere Straftaten.

Zu beachten ist allerdings, dass die Beschlagnahme in Redaktionsräumen bzw. in der Wohnung von Journalisten ohnehin nur in seltenen Ausnahmefällen zulässig ist (§ 97 Abs. 5 StPO).

2.3 Beschluss des Bundesarbeitsgerichts vom 14. Dezember 2005 (1 ABR 34/03) zur Videoüberwachung von Mitarbeitern

Zu entscheiden hatte das Bundesarbeitsgericht den Fall der Videoüberwachung eines Verteilzentrums der Deutschen Post AG. Es stellte fest, dass die Überwachung der Arbeitnehmer am Arbeitsplatz durch eine Videoanlage einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht darstellt. Dieser Eingriff kann nur durch überwiegende schutzwürdige Belange des Arbeitgebers gerechtfertigt sein.

Im konkreten Fall reichten Postgeheimnis, das Eigentum der Postkunden und die wirtschaftlichen Interessen des Arbeitgebers nicht aus, um die Einschränkung der Arbeitnehmer durch eine bis zu 60 Stunden pro Woche dauernde Videoüberwachung in den nicht öffentlich zugänglichen Arbeitsräumen zuzulassen.

3. Sonstiges

- Missbräuchliche Nutzung der Daten aus Presseausweisen

Entsprechend der Richtlinie des Bundesinnenministeriums und der Konferenz der Innenminister/-senatoren aus dem Jahre 1993 ist die Privatadresse von Journalisten auf den bundeseinheitlichen Presseausweisen anzugeben. In der Vergangenheit kam es im Rahmen der politischen Berichterstattung insbesondere über rechtsradikale Gruppen wiederholt zu Problemen. Bei den Eingangskontrollen von Veranstaltungen wurden die Presseausweise kontrolliert und die Privatadresse darauf notiert. Das führte zu Listen missliebiger Journalisten im Internet und am Ende zu Bedrohungen. Im Arbeitskreis der Rundfunkdatenschutzbeauftragten wurde diskutiert, wie solche Gefährdungen von Journalistinnen und Journalisten zu verhindern sind. Eine Möglichkeit wäre, anstelle der Privatadresse die Adresse der Rundfunkanstalt bzw. des Verlages zu verwenden.

Der Vorsitzende des AK DSB hat in dieser Angelegenheit Kontakt zu Medienverbänden aufgenommen. Der Justitiar des Deutschen Journalistenverbandes, Herr Benno Pöppelmann, hat es übernommen, die Meinung der Innenministerkonferenz und der ausstellungsberechtigten Verbände zu unserem Vorschlag einzuholen.

III. Berlin/Brandenburg

1. Gesetzgebung

1.1 8. Rundfunkänderungsstaatsvertrag

Am 1. April 2005 ist der 8. Rundfunkänderungsstaatsvertrag in Kraft getreten. Die Landesverordnungen über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht, die in den letzten Jahren mehr und mehr voneinander abgewichen waren, wurden aufgehoben und das Befreiungsrecht einheitlich in den Rundfunkgebühren-Staatsvertrag integriert. Nunmehr sind nicht mehr die Sozialbehörden im Auftrag der Rundfunkanstalten, sondern die GEZ zentral für die Befreiung zuständig. Das Verfahren sollte dadurch vereinfacht werden, dass der beantragende Rundfunkteilnehmer gemäß § 6 Abs. 2 Rundfunkgebührenstaatsvertrag (RGebStV) das Vorliegen der Befreiungsvoraussetzungen durch die Vorlage be-

stimmter sozialer Leistungsbescheide (z.B. über Sozialhilfe oder Arbeitslosengeld II) im Original oder in beglaubigter Kopie nachzuweisen hat. Im Gegensatz zum bis dahin gültigen Befreiungsverfahren, das sich am tatsächlichen Einkommen des beantragenden Teilnehmers orientierte und entsprechend nachweis- und bearbeitungsintensiv war, sollten die Neuerungen für Entlastung bei allen Beteiligten sorgen.

Da auf den der GEZ vorzulegenden z. T. bis zu 16 Seiten umfassenden Bescheiden auch viele sensible Daten enthalten sind, die für die Befreiungsbearbeitung nicht benötigt werden, ist hier allerdings eine wenig datenschutzfreundliche Regelung entstanden – insbesondere auch deshalb, weil die GEZ zu Nachweiszwecken Kopien der vollständigen Bescheide vorhalten muss und diese dazu in ihr Datenverarbeitungssystem einscannet. Die von der GEZ in Zusammenarbeit mit den Rundfunkdatenschutzbeauftragten erarbeitete Lösung eines einfachen, einseitigen Befreiungsformulars, auf dem die Sozialleistungsträger das Vorliegen der Befreiungsvoraussetzungen nur zu bestätigen hätten, ist bislang an unannehmbaren finanziellen Forderungen der Behörden gescheitert.

Das gegenwärtige Verfahren ist allerdings unter Einbeziehung der Länder zurzeit Gegenstand von Verhandlungen zwischen der Bundesagentur für Arbeit und den Rundfunkanstalten.

Hierbei ist konkret Folgendes geplant:

Durch eine Anpassung der Software soll die Bundesagentur für Arbeit die für die Befreiung notwendigen Daten auf einem separaten zusätzlichen Blatt übernehmen und diese so genannte „Drittbescheinigung“ dem Arbeitslosengeldbescheid als zusätzliche Seite beifügen. Der Rundfunkteilnehmer fügt dann diese Drittbescheinigung seinem Antrag auf Befreiung von der Rundfunkgebühr bei und versendet diese Unterlagen an die GEZ. Dieses Verfahren spart die Erhebung nicht notwendiger Daten. Zurzeit wird die Machbarkeit eines solchen Konzepts geprüft.

Mit dem Inkrafttreten des 8. Rundfunkänderungsstaatsvertrages wurde auch § 8 Abs. 4 RGebStV wirksam, auf dessen Problematik ich bereits in meinem vergangenen Tätigkeitsbericht eingegangen bin.

Einige Landesdatenschutzbeauftragten kritisieren diese Vorschrift als zu unbestimmt und weit und sehen darin keine gültige Rechtsgrundlage für die Anmietung von Adressen von privaten Adresshändlern zum Zwecke des Mailings.

Der **rbb** hält in Übereinstimmung mit seiner Rechtsaufsicht daran fest, dass die Anmietung von Adressen zur Durchführung von mailing-Aktionen mit dem Datenschutzrecht vereinbar ist und dass dies durch § 8 Abs. 4 RGebStV klargestellt wird.

Unabhängig davon finden zur Zeit Verhandlungen zwischen den Ländern, den Rundfunkanstalten, den Rundfunkdatenschutzbeauftragten, und den Datenschutzbeauftragten der Länder statt, um hier eine Lösung zu finden, die den datenschutzrechtlichen Bedenken Rechnung trägt, aber gleichzeitig sicherstellt, dass diese wichtige Möglichkeit zur Erschließung der Rundfunkgebühren weiterhin bestehen bleibt.

Im Zusammenhang mit dem 8. Rundfunkänderungsstaatsvertrag halte ich eine Informationsschrift der Datenschutzbeauftragten von Brandenburg zum Thema „Datenschutz bei der GEZ“, die die Behörde auch in ihr Internet-Angebot eingestellt hat, für kontraproduktiv. Darin heißt es u. a., dass die GEZ die Nachweise über die Gewährung von Sozialleistung, vollständig speichert, „obwohl dies gegen das Datenschutzrecht verstößt“ (Ziffer 7 des Faltblatts). In Ziffer 2 derselben Informationsschrift wird darüber informiert, dass die Praxis der Anmietung von Adressen von privaten Adresshändlern zu Zwecken des Mailings nicht dem Datenschutzrecht entspreche. Immerhin wurde auf Intervention des **rbb** der Hinweis aufgenommen, dass die GEZ die Rechtsgrundlage hingegen als ausreichend betrachte. Der Passus zum Verfahren bei dem Antrag auf Befreiung von der Rundfunkgebührenpflicht ist hingegen nach wie vor unverändert und führt – wie zahlreichen Nachfragen bei der GEZ und beim **rbb** zeigen – zu erheblichen Irritationen unter den Rundfunkteilnehmern.

2. Sonstiges

Auf Landesebene hat es im Berichtszeitraum keine sonstigen Maßnahmen mit unmittelbaren Auswirkungen auf den **rbb** gegeben.

C. Datenschutz und Datensicherheit im rbb

I. Interne Regelungen

1. Datenschutz-Dienstanweisung

Seit dem 21. November 2005 ist die Datenschutz-Dienstanweisung des **rbb** in Kraft. Darin sind die überwiegend abstrakten Regelungen des rbb-Staatsvertrags und des Berliner Datenschutzgesetzes für den **rbb** konkretisiert und ergänzt.

Die auf der Grundlage von § 31 Abs. 8 der Geschäftsordnung erlassene Dienstanweisung bildet den Grundstein der internen Regelungen zum Datenschutz. Sie setzt den datenschutzrechtlichen Grundsatz der Datensparsamkeit konkret um. Danach ist der Umfang der im **rbb** außerhalb des journalistischen Bereichs zu verarbeitenden personenbezogenen Daten auf das erforderliche Minimum zu beschränken.

Die Dienstanweisung stellt klar, dass die Verantwortung für Datenschutz und Datensicherheit nicht nur bei den Verantwortungsträgern und bei den für die Technik zuständigen Bereichen, sondern auch bei jeder einzelnen Kollegin und jedem einzelnen Kollegen liegt.

Für jedes System, mit dem personenbezogene Daten verarbeitet werden, ist ein Konzept zur Gewährleistung von Datenschutz und Datensicherheit erforderlich. Systeme für die Verarbeitung von Personaldaten und solche, die technisch dazu geeignet sind, eine Leistungs- und Verhaltenskontrolle zu ermöglichen, dürfen generell erst nach einer Vorabkontrolle durch die Datenschutzbeauftragte eingeführt werden.

2. Dienstvereinbarung über die Einführung und Anwendung des Telekommunikationsanlagenverbundes und Dienstvereinbarung über die Nutzung mobiler Telekommunikationsgeräte

Im Dezember 2005 hat der **rbb** eine neue Telefonanlage in Betrieb genommen. Für die Nutzung der Telefonanlage und für die Abrechnung der Telefongebühren bedarf es einer Regelung. Das gleiche gilt für die Nutzung und Abrechnung von Mobilfunk.

Für beide Gerätearten – Festnetz und Handy - werden derzeit Entwürfe für Dienstvereinbarungen erarbeitet. Daran bin ich maßgeblich beteiligt.

Vorrangiges Ziel der Dienstvereinbarungen ist der Schutz personenbezogener Daten und der Schutz des nicht öffentlich gesprochenen Wortes. In den Vereinbarungen wird jeweils festgelegt, welche Funktionen und Leistungsmerkmale genutzt werden dürfen. Außerdem wird im Einzelnen aufgelistet, welche personenbezogenen Daten für welche Zwecke auf welche Weise verarbeitet werden.

3. Dienstanweisung für den Einsatz von externen Firmen bei der Wartung von IT-Systemen

Der Einsatz von externen Firmen bei der Wartung von IT-Systemen birgt Gefahren für den Schutz personenbezogener Daten und für die Datensicherheit in sich. Das gilt insbesondere dann, wenn dem Fremdpersonal Zugang zum Hausnetz gewährt werden muss.

In § 3a Berliner Datenschutzgesetz, der über § 36 **rbb**-Staatsvertrag Anwendung findet, sind für die sog. Fremdwartung spezielle Anforderungen geregelt.

Die darin enthaltenen abstrakten Regelungen dienen insbesondere dazu, eine umfassende Kontrolle der Wartungsarbeiten durch den Auftraggeber sicherzustellen. Außerdem soll ausgeschlossen werden, dass bei der Wartung Programme und Daten aufgerufen werden können, die für die Arbeit nicht benötigt werden.

Zusammen mit dem IT-Sicherheitsbeauftragten aus der Abteilung Informations- und Kommunikationstechnik, Herrn Gerry Wolff, und einem Kollegen aus der Abteilung Organisation und betriebswirtschaftliche IT-Systeme habe ich einen Entwurf

für eine Dienstanweisung für den Einsatz externer Firmen bei der Wartung von IT-Systemen erarbeitet.

Unter Wartung wird die Summe aller Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen verstanden; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie Pflege, Überprüfung und Reparatur oder der Austausch von Hardware.

Ich habe den Entwurf vor kurzem der Intendantin zugeleitet und hoffe, dass demnächst eine entsprechende Dienstanweisung erlassen wird.

II. Aktuelle IT-Projekte

1. Service Desk beim rbb

Der **rbb** verfügt über ca. 2500 PC Arbeitsplätze an den Standorten Berlin, Potsdam, Frankfurt/Oder, Prenzlau und Perleberg. Auf diesen Systemen werden unterschiedliche Betriebssysteme und Software sowie rundfunkspezifische Applikationen eingesetzt.

Im Herbst 2005 wurden die beiden bisher zuständigen Supporteinheiten in Berlin und Potsdam, die für die Betreuung der Standard PC-Arbeitsplätze zuständig sind, zusammengelegt. Dabei wurde ein ServiceDesk entsprechend der Information Technology Infrastructure Library (ITIL) implementiert, der sich in ein Front- und Back-Office unterteilt. Das Front-Office wurde zentral in Berlin etabliert und ist für den Telefonsupport zuständig. Das Back-Office ist standortbezogen in Berlin und Potsdam vorhanden. Als 2nd Level Support wurden bereits die Bereiche Netzwerk und Server integriert.

Zusätzlich wurde ein neues, einheitliches Service-Desk-System ausgewählt und eingeführt. Im Rahmen der von mir durchgeführten Vorabkontrolle konnte ich mich davon überzeugen, dass

- ? nur diejenigen Daten der Mitarbeiterinnen und Mitarbeiter des Service Desks und der Anfragenden in dem System verarbeitet werden, die für den Service erforderlich sind,
- ? es ein praktikables Berechtigungskonzept gibt,
- ? angemessene Löschfristen gelten,
- ? ausschließlich anonyme Auswertungen durchgeführt werden und
- ? dass es keine Schnittstellen zu anderen Systemen gibt.

2. Neues Redaktions- und Sendesystem für rbbtext

Mit einem neuen Redaktions- und Sendesystem ist **rbbtext** am 26. Oktober 2005 auf Sendung gegangen. Die neue Anlage macht **rbbtext** fit für das Digitalfernsehen. Sie wurde, um Kosten zu sparen und technische Synergien nutzen zu können, gemeinsam mit der Redaktion ARD-Text beschafft, die den Teletext für das Erste sendet. Das System eröffnet für die Zukunft die Möglichkeit der Produktion von Teletext und Textdiensten für das Digitalfernsehen auf demselben System und das Ausspielen der Seiten in den jeweils dafür benötigten Standards. Der **rbb** ist der erste Sender im deutschsprachigen Raum, der diese moderne Technik einsetzt.

Das Redaktions- und Sendesystem basiert auf einem zentralen Server, über Netzwerk angeschlossenen Arbeitsplatz-PCs und mehreren Ausspielrechnern, die die sendefertigen Beiträge in das Fernseh-Signal eintasten. Für den Havarie-Fall springen automatisch Ersatz-Rechner ein, die die ganze Zeit auch das System überwachen.

Ich habe mich im Rahmen der von mir durchgeführten Vorabkontrolle davon überzeugt, dass die für das System erforderlichen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit ergriffen worden sind. Den Zugriff auf das System regelt eine Benutzerverwaltung, die von der Redaktion organisiert wird. Die einzi-

gen Personen, die Zugriff haben, aber nicht zur Redaktion gehören, sind die System-Administratoren des **rbb** sowie über einen gesicherten Zugang von außen die beiden Systemverantwortlichen der Herstellerfirma. Als Begleitdaten zu einem Beitrag werden nur die Nutzerkürzel und die Uhrzeit sowie das Datum der Erstellung mitgeführt. Auch werden letzte Änderungen protokolliert. Mit Ablauf der Archivfrist werden sämtliche Daten gelöscht.

3. Software für Projektmanagement

Zur Planung und Fortschreibung der Hörfunk-, Fernseh- und IT-Projekte der Produktions- und Betriebsdirektion ist im Februar 2006 eine datenbankbasierte Software zum Thema „Multi-Projektmanagement“ eingeführt worden. Dieses neue System dient der Verbesserung der Planungseffizienz und der konfliktfreien Zuordnung der Ressourcen zu Projektaufgaben. Die Planungsergebnisse sind eine Grundlage für die jährliche bzw. mittelfristige Wirtschaftsplanung.

Verarbeitet werden in dem System lediglich folgende Daten:

- ? der Name und die Zuordnung der Person zu einer Funktionseinheit,
- ? Abwesenheitszeiten auf Tagesebene ohne weitere Spezifikation der Abwesenheitsgründe und
- ? Zuordnung der Person zu Projektaufgaben mit Starttermin (Planwert) und Endtermin (Planwert).

Da personenbezogene Ist-Daten nicht erfasst werden, kann keine Leistungs- und Verhaltenskontrolle durch das System stattfinden. Durch ein Berechtigungskonzept ist sichergestellt, dass lediglich diejenigen Personen lesenden und/oder schreibenden Zugriff auf das System haben, die dies für ihre Aufgaben benötigen.

4. Digitales Produktionssystem Fernsehen

Im März 2006 ist beim **rbb** ein Digitales Produktionssystem in Betrieb gegangen. Dieses neue System soll ein vernetztes Arbeiten der Redaktionen 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 verbessert werden, damit der Redaktionsschluss näher an den Ausstrahlungszeitpunkt des Beitrages gelegt werden kann. Das Videomaterial wird während der Produktion nicht mehr physisch auf Videobändern gespeichert, kopiert und umher transportiert, sondern liegt als Datenfile vor und wird über ein Netzwerk durch das Haus und über Standortgrenzen hinweg transportiert.

In dem System werden das Videomaterial und die dazugehörigen Metadaten gespeichert. Die Zugriffe auf das System werden durch ein Berechtigungskonzept gesteuert. Dadurch und durch weitere technische und organisatorische Maßnahmen ist insbesondere die Integrität (Unversehrtheit) des Materials sichergestellt.

Es werden keine Nutzerevents als Historie im System gespeichert. DPS protokolliert lediglich die letzte Aktualisierung von Videomaterial und versieht sie mit einem Zeitstempel. Nur über diesen Zeitstempel könnte man im Logfile herausfinden welche Person eine Zuordnung durchgeführt hat.

III. Arbeitnehmerdatenschutz

1. Datenschutz bei digitalen Kopiergeräten

Moderne Kopiergeräte verfügen über eingebaute Festplatten, auf denen dauerhaft die Originale quasi als „Foto“ gespeichert werden können. Im Zuge der üblichen Wartungsarbeiten können diese Dokumente in den Zugriff der (externen) Techniker geraten. Dasselbe gilt, wenn die Geräte (oft handelt es sich um Leasinggeräte) ausgetauscht oder zu einer Reparatur außer Haus gegeben werden, ohne dass die Festplatte zuvor gelöscht wird.

Für derartige Geräte bieten die Hersteller inzwischen ein sog. Daten-Sicherheits-Kit (SD-Karte) an, mit dem alle auf der Festplatte temporär gespeicherten Daten mehrmals mit Daten überschrieben werden, so dass sie nicht mehr rekonstruierbar sind.

Mit der Abteilung Einkauf und Logistik habe ich vereinbart, dass sämtliche Kopierer mit Festplatte – dort wo dies möglich ist - mit einem Security Kit nachgerüstet werden. Bei Neuanschaffung von Kopiersystemen wird darauf geachtet, dass die Geräte von vornherein mit einem Security Kit ausgestattet sind.

Diejenigen Nutzerinnen und Nutzer der beiden im **rbb** befindlichen Geräte mit Festplatte, die nicht mit einem Security Kit nachgerüstet werden können, wurden darüber belehrt, wie sie verhindern können, dass Datenmaterial längerfristig auf der Festplatte gespeichert wird. Bei Austausch bzw. Rückgabe dieser Geräte werden unter meiner Aufsicht die Festplatten gelöscht und dieser Vorgang in einem Übergabeprotokoll festgehalten.

2. Rahmenvereinbarung der ARD-Anstalten und des ZDF mit einer Buchungsfirma über das Dienstreiseaufkommen für ARD/ZDF

Um das Dienstreiseaufkommen noch effizienter und wirtschaftlicher abzuwickeln, hat der **rbb** federführend für die anderen ARD-Anstalten und dem ZDF eine Rahmenvereinbarung mit einer Buchungsfirma abgeschlossen. Zur Auftragsabwicklung sieht die Vereinbarung eine Speicherung der Profile der Rundfunkanstalten und der Reisenden vor. Ich habe sichergestellt, dass die zu speichernden personenbezogenen Daten der Reisenden auf den erforderlichen Umfang begrenzt werden. Außerdem ist auf meine Initiative die Geheimhaltungsklausel verstärkt worden. Schließlich ist ausdrücklich aufgenommen worden, dass Reisende jederzeit Auskunft über ihre Daten oder deren Berichtigung verlangen können. Die Reisenden haben die Möglichkeit, der dauerhaften Speicherung ihres Reisendenprofils bei der Buchungsfirma zu widersprechen.

3. Rahmenvereinbarung der ARD-Anstalten und des ZDF mit einer Hotelreservierungsgesellschaft

Um die vorteilhaften Konditionen von Großkunden auf dem Reisesektor auch bei Hotelbuchungen nutzen zu können, hat der SWR federführend für die ARD und das ZDF eine Rahmenvereinbarung mit einer Hotelreservierungsgesellschaft abgeschlossen. Diese Vereinbarung ermöglicht den Mitarbeitern, ihre Zimmer für Dienstreisen selbst online zu reservieren, ohne die Reisedienstellen des Hauses bemühen zu müssen.

In den Rahmenvertrag sind Datenschutzbestimmungen aufgenommen worden, die die Einhaltung der gesetzlichen Datenschutzregelungen gewährleisten. Bei sämtlichen Vorgängen mit personenbezogenen Daten (Erhebung, Verarbeitung, Nutzung) dürfen die Daten nur im Rahmen der Weisungen der Rundfunkanstalten verwendet werden. Eine Nutzung und Weitergabe für andere Zwecke ist unzulässig. Der Vertrag unterbindet personenbezogene Auswertungen über die Reisenden und erlaubt nur anonyme Statistiken. Darüber hinaus schreibt der Vertrag das Kontrollrecht der jeweiligen Rundfunkdatenschutzbeauftragten fest und enthält die Maßgabe, alle notwendigen technischen und organisatorischen Maßnahmen zur Datensicherheit zu treffen.

4. Fahrzeugdispositions-Software in der HA Finanzen und Logistik

Im Frühjahr 2006 ist im Bereich Logistik ein Software-Produkt eingeführt worden, mit welchem zukünftig die firmeneigenen Fahrzeuge Kosten sparend und zentral disponiert werden sollen.

Mittelfristig ist auch geplant, dass jede Mitarbeiterin/jeder Mitarbeiter eine Fahrzeuganforderung direkt über das Intranet veranlassen kann. Dazu werden dem neuen System die notwendigen personenbezogenen Daten wie Name und Kostenstelle aus dem SAP-System und aus dem Datenbestand der Abteilung IuK zur Verfügung gestellt. Diese Daten dienen dazu, den Anforderungsprozess über das Intranet zu gewährleisten, personenbezogene Auswertungen sind nicht vorgesehen.

Auf meine Initiative wurde ein differenziertes Berechtigungskonzept eingeführt und die regelmäßige Löschung sämtlicher personenbezogener Daten aus dem System nach jeweils 2 Jahren vorgesehen.

5. Zugriff des Empfangspersonals auf das im Intranet bereitgestellte Telefonbuch aller Mitarbeiterinnen und Mitarbeiter

Im Juni 2006 wurde ich über Planungen der Abteilung Infrastruktur informiert, den Mitarbeiterinnen und Mitarbeitern an den Empfängen des **rbb** einen Zugriff auf das im Intranet vorgehaltene Telefonbuch einzuräumen. Neben den Telefonnummern enthält das Telefonbuch auch die E-Mail-Adressen der Mitarbeiterinnen und Mitarbeiter und die Raumnummern, in denen die Mitarbeiterinnen und Mitarbeiter sitzen.

Nachdem ich mich von der Erforderlichkeit des Zugriffs durch das Empfangspersonals vergewissert hatte, habe ich dem Projekt unter der Bedingung zugestimmt, dass von sämtlichen Mitarbeiterinnen und Mitarbeitern am Empfang – wie mit dem Sicherheitsunternehmen auch vertraglich vereinbart – eine Vertraulichkeitserklärung vorgelegt wird. Dies ist inzwischen geschehen.

6. Mitarbeiter-Umfragen im Intranet

Unter Nutzung eines Tools von Lotus Notes werden beim **rbb** zunehmend anonyme Umfragen z.B. zum Bedarf an Kinderbetreuung während der Schulferien oder zur Qualität der Kantinen durchgeführt. Ich habe mich von der Gewährleistung der Anonymität der Umfragen überzeugen können.

IV. Sonstiges

1. Verpflichtung auf das Datengeheimnis der freien Mitarbeiterinnen und Mitarbeiter

Zusammen mit der HA Personal habe ich eine Verschwiegenheitsklausel erarbeitet, die künftig in allen Rahmenverträgen mit den freien Mitarbeiterinnen und Mitarbeitern enthalten sein wird.

Außerdem werden alle freien Mitarbeiterinnen und Mitarbeiter, die personenbezogene Daten verarbeiten, künftig noch eine spezielle datenschutzrechtliche Verpflichtungserklärung unterzeichnen.

2. Schulungen

Auch im Berichtsjahr habe ich wieder mehrere Datenschutzs Schulungen für Kolleginnen und Kollegen durchgeführt. Eine Zielgruppe waren beispielsweise die neuen Auszubildenden.

D. Datenschutz bei der Rundfunkteilnehmer-Datenverarbeitung

I. Allgemeines

Die Gebühreneinzugszentrale in Köln (GEZ) ist das gemeinsame Rechenzentrum von ARD, ZDF und DeutschlandRadio. Sie verarbeitet die Rundfunkteilnehmerdaten für die Landesrundfunkanstalten als Auftragnehmer im datenschutzrechtlichen Sinn (§ 8 Abs. 2 RGebStV). Hier werden auch die Daten der Rundfunkteilnehmer im Sendegebiet des **rbb** verarbeitet.

Die GEZ erhebt, verarbeitet und nutzt die personenbezogenen Teilnehmerdaten ausschließlich zum Zweck des Gebühreneinzugs. Für die Datenschutzkontrolle ist jeweils der Rundfunkdatenschutzbeauftragte der einzelnen Anstalten für seinen Teilnehmerkreis zuständig. In den Ländern Berlin und Brandenburg, Bremen und Hessen üben die staatlichen Datenschutzbeauftragten diese Kontrollfunktion aus.

Routinemäßige Datenschutzaufgaben werden gemäß § 8 Abs. 2 RGebStV von der betrieblichen Datenschutzbeauftragten der GEZ, Frau Kerstin Arens, vor Ort in Köln wahrgenommen. Mit ihr stehe ich in ständigem Austausch. Als Mitglied des Arbeitskreises der Rundfunkdatenschutzbeauftragten ist sie in das Netzwerk der Rundfunkdatenschutzbeauftragten eingebunden.

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

In der Zeit vom 21. bis 23. September 2004 ist die GEZ von den Datenschutzbeauftragten der Länder Hessen, Bremen, Berlin und Brandenburg geprüft worden.

Im Juni 2005 ging den Rundfunkanstalten der gemeinsame Prüfbericht der Landesdatenschutzbeauftragten zu.

Wie bereits die Diskussionen im Vorfeld erwarten ließen, vertraten die Landesdatenschutzbeauftragten darin die Auffassung, dass es keine gesetzliche Grundlage

für die Durchführung der Mailing-Maßnahmen der GEZ gebe. Auch § 8 Abs. 4 RGebStV biete keine hinreichende Rechtsgrundlage. Die ständige Praxis der GEZ, nicht zustellbare Anschriften zur Geltendmachung von Gewährleistungsansprüchen an die Adresshändler zurückzumelden, sei unzulässig. Auch der Inhalt der Mailingschreiben wurde kritisiert. So sei in einigen Musterschreiben beispielsweise der Hinweis auf die Freiwilligkeit bestimmter Angaben nicht deutlich genug.

Die Landesdatenschutzbeauftragten bezweifeln die Notwendigkeit einer Zugriffsmöglichkeit für jede Sachbearbeiterin und jeden Sachbearbeiter bei der GEZ auf sämtliche Teilnehmerkonten in Deutschland. Für die Rundfunkgebührenbeauftragten wird diese Zugriffsmöglichkeit erst recht abgelehnt. Nach Auffassung der Landesdatenschutzbeauftragten weise zudem die in § 8 Abs. 3 Satz 2 RGebStV vorgeschriebene Protokollierung des Abrufs von Teilnehmerdaten von nicht zuständigen Rundfunkanstalten Mängel auf.

Mit Schreiben vom 17. Februar 2006 hat die Intendantin die gemeinsame Stellungnahme der von der Prüfung unmittelbar betroffenen Rundfunkanstalten dem Berliner Beauftragten für Datenschutz und Informationsfreiheit übermittelt. An der Erarbeitung der Stellungnahme habe ich intensiv mitgewirkt.

Die Rundfunkanstalten haben darin noch einmal ausführlich dargelegt, dass und warum sie § 8 Abs. 4 RGebStV für eine geeignete Rechtsgrundlage für die Anmietung von Adressen bei privaten Adresshändlern zur Durchführung von Mailing-Maßnahmen halten (s. dazu auch mein 2. Tätigkeitsbericht, 7 ff.). Nach Auffassung der Rundfunkanstalten stellt die Rückübermittlung von Anschriften an die Adresshändler bereits keine Verarbeitung personenbezogener Daten im Sinne der Datenschutzgesetze dar. Dem Adresshändler wird lediglich mitgeteilt, dass ein Schreiben der GEZ an der gelieferten Anschrift nicht zugestellt werden konnte. Daraus kann nichts über die Person des Betroffenen geschlossen werden. Allein die bloße Möglichkeit, dass der Betroffene an der angegebenen Adresse nicht wohnt, macht die Mitteilung noch nicht zu einem personenbezogenen Datum. Die Rückübersendung von Adressen zur Geltendmachung von Gewährleistungsansprüchen ist für die zur

Sparsamkeit und Wirtschaftlichkeit gesetzlich verpflichteten Rundfunkanstalten auch erforderlich und verhältnismäßig.

Die Musterbriefe, die bei den Mailingmaßnahmen verwendet wurden, und deren Wortlaut leider nicht – wie in der Vergangenheit üblich – zuvor mit den Mitgliedern des AK DSB abgestimmt worden waren, wurden inzwischen überarbeitet. Der Hinweis darauf, wann keine Pflicht zur Beantwortung der Briefe besteht (dann wenn keine Rundfunkempfangsgeräte zum Empfang bereitgehalten werden), erfolgt jetzt wieder deutlich.

Ich habe darum gebeten, dass künftig wieder sämtliche datenschutzrechtlich relevanten Modifizierungen der in Berlin und Brandenburg verwendeten Musterbriefe, vor dem Einsatz mit mir abgestimmt werden.

Schon in den Vorbesprechungen mit den Landesdatenschutzbeauftragten zum Prüfbericht bestand Einvernehmen mit den Landesdatenschutzbeauftragten, dass derzeit keine sinnvolle Abgrenzung der Zugriffsrechte (z. B. nach Bundesländern oder aufgrund alphabetischer Zuordnung) der Sachbearbeiterinnen und Sachbearbeiter der GEZ denkbar erscheint, durch die die Abwicklung der schriftlichen und insbesondere der telefonischen Sachbearbeitung bei der GEZ nicht in unververtretbarem Maße beeinträchtigt würde, und zwar auch zum Nachteil eines kundenfreundlichen Services.

Jährlich müssen hunderttausende von Umzügen von Teilnehmern aus dem Zuständigkeitsbereich einer Landesrundfunkanstalt in einen anderen im Bestand nachvollzogen werden. Dabei kommt es häufig vor, dass Sachverhalte zwischen den Rundfunkanstalten und der GEZ zu klären, zu verändern oder zu ergänzen sind. Ähnliche Probleme ergeben sich bei Teilnehmern mit mehreren Wohnsitzen.

Alle Zugriffsnotwendigkeiten auf Teilnehmerkonten anderer Landesrundfunkanstalten ergeben sich auch bei der Tätigkeit der Rundfunkgebührenbeauftragten. Hier kommen allerdings noch weitere Faktoren hinzu:

Die Beauftragten können die Online-Abfrage, die über sichere Übertragungswege erfolgt, für die Vor- und Nachbearbeitung ihrer Touren einsetzen. Die Zugriffsmöglichkeit allein auf den Bezirk des jeweiligen Gebührenbeauftragten zu beschränken, hieße, die Effizienz des gesamten Systems wesentlich einzuschränken. Sachverhalte ließen sich nur zu einem geringen Teil vollständig aufklären, da eine Registrierung bei einer anderen Landesrundfunkanstalt außer Betracht bleiben müsste. Im Übrigen könnten falsche, unvollständige oder widersprüchliche Aussagen nicht entlarvt werden.

Die Protokollierung der „Fremdzugriffe“ gemäß § 8 Abs. 3 RGebStV ist - entgegen der Ansicht der Landesdatenschutzbeauftragten - auch schon bislang korrekt erfolgt. Sie enthielt auch schon bislang sämtliche erforderlichen Daten. Das betrifft insbesondere auch den Zugriffsgrund. Allerdings hatte sich der den Leiterinnen und Leitern der Rundfunkgebührenstellen zu Kontrollzwecken zur Verfügung gestellte Ausdruck auf einen Teil dieser Daten beschränkt. Es wurde veranlasst, dass den Rundfunkgebührenstellen zukünftig wieder ein vollständiger Ausdruck zur Verfügung gestellt wird.

Im Jahresbericht 2005 des Berliner Beauftragten für Datenschutz und Informationsfreiheit und im Tätigkeitsbericht der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg für die Jahre 2004 und 2005 wurden jeweils die Ergebnisse der datenschutzrechtlichen Prüfung der GEZ dargestellt, ohne die Stellungnahme der Rundfunkanstalten zu dem gemeinsamen Prüfbericht zu erwähnen. Möglicherweise lag zum Zeitpunkt des Redaktionsschlusses die Stellungnahme der Rundfunkanstalten noch nicht vor. Zumindest hätte dann aber m. E. ein Hinweis auf die noch ausstehende Stellungnahme der Rundfunkanstalten in den Berichten erfolgen müssen.

III. Neues Löschkonzept

Das bislang gültige Löschkonzept für die Daten der Teilnehmerhistorie datiert aus dem Jahr 1995. Seinerzeit waren unter Einbindung der Gebührenabteilungen und der Datenschutzbeauftragten der Rundfunkanstalten die so genannten Fundamen-

tal-Funktionscodes festgelegt worden, die im Teilnehmerkonto enthalten bleiben, solange das Konto besteht (z. B. die Anmeldung). Für alle übrigen Funktionscodes wurden gemäß den gesetzlichen Vorgaben Löschrufen definiert.

Da das ab 11. Juli 2005 in Betrieb genommene neue DV-System keine Funktionscodes mehr kennt, sondern mit dem Begriff der Geschäftsvorfälle arbeitet, von denen zudem weitaus mehr existieren, als seinerzeit Funktionscodes vorhanden waren, bedarf es einer Überarbeitung des Löschkonzeptes.

Am 21. Oktober 2005 hat sich eine Unterarbeitsgruppe des AK DSB, der ich angehöre, zusammen mit Mitarbeiterinnen und Mitarbeitern der GEZ mit der bisherigen Liste der Funktionscodes bzw. den entsprechend im Neusystem vorhandenen Geschäftsvorfällen befasst. Es wurde festgestellt, dass eine Reihe der bisher als Fundamental-Funktionscodes eingestuft Daten nicht mehr unbefristet gespeichert werden müssen, sondern nach kürzeren Zeiträumen gelöscht werden können.

Eine endgültige Abstimmung des Löschkonzeptes, insbesondere hinsichtlich der weitergehenden Geschäftsvorfälle, steht derzeit noch aus. Das endgültige Konzept befindet sich noch im Stadium der Erarbeitung bei der GEZ.

IV. Neue Richtlinien für den Datenschutz bei der GEZ

Am 1. Februar 2006 ist bei der GEZ eine aktualisierte Fassung der Datenschutzrichtlinien in Kraft getreten, die mit allen Rundfunkdatenschutzbeauftragten zuvor abgestimmt worden war. Darin wird insbesondere den veränderten technischen Anforderungen an die Datensicherheit Rechnung getragen. Außerdem wird in einem eigenen Kapitel auf den Umgang mit personenbezogenen Daten bei der Anmietung von Adressen bei privaten Adresshändlern für die sog. Mailing-Maßnahmen eingegangen.

V. NP-Datenbank bei der GEZ

In einer Sondersitzung bei der GEZ wurde dem Arbeitskreis der Rundfunkdatenschutzbeauftragten (AK DSB) am 7. November 2005 erstmalig ein neues Projekt

der GEZ vorgestellt. Geplant ist die Errichtung einer sog. NP (NichtPrivate)-Datenbank, in der ausschließlich die Daten von Unternehmen enthalten sein sollen. Zu den Unternehmen gehören nicht nur juristische Personen, sondern zum Beispiel auch die Angehörigen freier Berufe und Kaufleute. Zweck der Datenbank ist die bessere und systematische Ausschöpfung des nichtprivaten Marktes. Sie soll zur Vernetzung verschiedener Marktinstrumente (z. B. Mailing, Beauftragtendienst etc.) verwendet werden.

Der AK DSB hielt die in der Sitzung präsentierte Version des Projekts, bei der die dauerhafte Speicherung auch von Nichtteilnehmern vorgesehen war, mit großer Mehrheit (ich gehörte auch dazu) für datenschutzrechtlich nicht vertretbar. Inzwischen haben weitere Besprechungen mit dem Ziel stattgefunden, zu datenschutzkonformen Lösungen zu kommen. Die Gespräche dauern weiter an.

VI. Datenschutzverstoß bei einem externen Dienstleister

Mitte November 2005 erhielt die GEZ durch die Mitteilung eines Mitarbeiters einer Drittfirma Hinweise auf einen Datenschutzverstoß bei einem externen Dienstleister der GEZ. Danach war der Vertragspartner der GEZ bzw. der Subunternehmer, der sich mit einer anderen Firma das Betriebsgelände teilt, den vertraglich vereinbarten Auflagen zu einer datenschutzgerechten Aufbewahrung und Entsorgung der bis zum Umstieg auf DV2005 zu bearbeitenden Papierbelege nicht nachgekommen. Der Subunternehmer hatte die Papierbelege nicht, wie vertraglich gefordert, in verschlossenen Alucontainern auf dem Betriebsgelände gelagert, sondern in zwar verschließbaren, aber leicht zu öffnenden Plastikcontainern, aus denen ohne Schwierigkeiten Dokumente entnommen werden konnten. Der unmittelbare Vertragspartner der GEZ, der seinerseits die Einhaltung der datenschutzrechtlichen Vorgaben vertraglich garantiert hatte, war seinen Kontrollpflichten nicht nachgekommen. Nach Bekanntwerden des Vorfalls hat der Geschäftsführer der GEZ die Revision mit einer Untersuchung der Vorgänge beauftragt. Dabei wurden weitere Schwachstellen offenbar.

Die Geschäftsleitung hat den Verwaltungsrat der GEZ und den Arbeitskreis der Datenschutzbeauftragten unmittelbar nach Abschluss der Aufklärung über die festgestellten Vorgänge und das geplante weitere Vorgehen informiert.

Als Konsequenz aus dem Vorgang wurde mit dem Vertragspartner ein Aufhebungsvertrag mit Wirkung zum Ende des 1. Quartals 2006 geschlossen. Außerdem wurde veranlasst, dass es zukünftig keine Verträge im Rahmen der Auftragsdatenverarbeitung mehr geben wird, bei denen die eigentliche Bearbeitung von einem Subunternehmer durchgeführt wird, oder an denen ein Subunternehmer maßgeblich beteiligt ist.

VII. DV 2005

Das neue Datenverarbeitungssystem bei der GEZ „DV 2005“ ist am 11. Juli 2005 in Betrieb genommen worden.

Es unterliegt nach wie vor der Prüfung durch die Revision der GEZ. Außerdem prüfen derzeit auch die betriebliche Datenschutzbeauftragte der GEZ und der Datenschutzbeauftragte des SWR, Herr Prof. Armin Herb, einzelne Teilaspekte des neuen Systems (z. B. die Auskunftsmasken).

VIII. Anfragen und Beschwerden

Sowohl bei der GEZ als auch direkt beim **rbb** gehen regelmäßig zahlreiche Anfragen und Beschwerden von Rundfunkteilnehmern mit datenschutzrechtlicher Relevanz ein. Die Datenschutzbeauftragten der Rundfunkanstalten haben die Bearbeitung und Beantwortung von Anfragen und sonstigem Routineschriftwechsel in Datenschutzangelegenheiten der GEZ übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter und von individuellen Anfragen mit besonderer datenschutzrechtlicher Bedeutung haben wir uns selbst vorbehalten.

Auch in diesem Jahr hatte ich hauptsächlich wieder Anfragen nach der Herkunft der bei der GEZ vorhandenen Daten zu beantworten. Vereinzelt gab es auch Beschwerden, deren Ursache hauptsächlich in der starken Überlastung der Sachbear-

beitung der GEZ durch den Bearbeitungsrückstau im Befreiungswesen zu suchen war. Allen Beschwerden konnte abgeholfen werden.

IX. Datenschutz und Datensicherheit bei den Rundfunkgebührenbeauftragten

Im Januar 2006 habe ich wieder gemeinsam mit dem Systemverantwortlichen für IT-Sicherheit, Herrn Gerry Wolff, zwei datenschutzrechtliche Schulungen mit den Rundfunkgebührenbeauftragten durchgeführt. Aus Anlass der veränderten technischen Bedürfnisse und Möglichkeiten, haben wir gemeinsam mit dem Leiter der Rundfunkgebührenstelle die für die Beauftragten die geltenden datenschutzrechtlichen Vorgaben aktualisiert.

E. Datenschutz im Informationsverarbeitungszentrum (IVZ)

Im Rahmen des routinemäßigen Austausches über datenschutzrechtliche Themen fanden am 9. Juni 2005 und am 22. März 2006 jeweils Besprechungen der Rundfunkdatenschutzbeauftragten der Betreiberanstalten MDR, NDR, SR, DLR, RB und **rbb** mit dem Geschäftsführer des gemeinsamen Informationsverarbeitungszentrums (IVZ), Herrn Dr. Georg Greten, statt.

Das IVZ strebt eine Zertifizierung hinsichtlich der Einhaltung datenschutz- und datensicherheitsrechtlicher Bestimmungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) an. Die Zertifizierung wird jeweils auf zwei Jahre befristet ausgesprochen. Im Zusammenhang mit den Vorbereitungsarbeiten soll auch die seit langem seitens der Rundfunkdatenschutzbeauftragten eingeforderte Aktualisierung des Datensicherheitskonzepts des IVZ vorgenommen werden. Die Rundfunkdatenschutzbeauftragten haben darauf hingewiesen, dass die Zertifizierung ihre Forderungen nicht ersetzt. Es wurde vereinbart, dass wir in die Vorbereitungen einbezogen werden.

Durch einen Beschluss des IVZ-Verwaltungsrates ist klargestellt, dass die internen Regelungen des **rbb** als Sitzanstalt auch für das IVZ entsprechend gelten. Damit ist sichergestellt, dass beispielsweise die Datenschutz-Dienstanweisung und die Dienstanweisungen zur Nutzung von Internet und E-Mail und zur Nutzung von Lotus Notes (letztere mit leichten Modifikationen, weil beim IVZ ein anderes Mail-System zum Einsatz kommt) auch beim IVZ Anwendung finden.

Beim IVZ sind im Berichtsjahr einige Teleheimarbeitsplätze für SAP-Entwickler entstanden. Die datenschutzrechtlichen Anforderungen dafür wurden von den Rundfunkdatenschutzbeauftragten vorgegeben.

F. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Im Berichtszeitraum hat der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR zwei ordentliche Sitzungen – am 13./14. Oktober 2005 beim NDR in Hamburg und am 23./ 24. März 2006 beim Deutschlandradio in Berlin – durchgeführt.

Auf der Hamburger Sitzung hat sich der Arbeitskreis mit den aktuellen Entwicklungen in der Gesetzgebung und Rechtsprechung beschäftigt und zahlreiche Einzelthemen wie z.B. der Einhaltung des Datenschutzes bei der Messung der Nutzungszahlen der Online-Angebote, mit der Verarbeitung personenbezogener Daten in Auslandsstudios, mit dem Inhalt von Drehgenehmigungsverträgen usw. beschäftigt.

Am zweiten Tag waren die Landesdatenschutzbeauftragten aus Hamburg, Schleswig-Holstein, Mecklenburg-Vorpommern und Niedersachsen zu Gast. Es fand ein reger Gedankenaustausch zur Rundfunkteilnehmerdatenverarbeitung, insbesondere zur Praxis der Gebührenbefreiung statt.

Der Datenschutzbeauftragte des WDR, Herr Thomas Drescher, wurde auf der Sitzung in Nachfolge des Datenschutzbeauftragten des SWR, Herrn Prof. Dr. Armin Herb, für die Dauer von zwei Jahren zum Vorsitzenden des AK DSB gewählt. Ich wurde in meinem Amt als stellvertretende Vorsitzende des AK DSB für zwei weitere Jahre bestätigt.

Auf unserer Sitzung am 23./24. März 2006 in Berlin konnten wir die Kolleginnen des Österreichischen Rundfunks ORF, Frau Wesey, und des Schweizer Rundfunks SRG SSR idée suisse, Frau Wenninger, in unserer Runde begrüßen. Wir konnten uns darüber informieren, wie der Einzug der Rundfunkgebühren in Österreich und in der Schweiz organisiert ist, und uns über die Organisation der Datenschutzkontrolle austauschen. Außerdem haben wir wieder eine Reihe von Einzelthemen erörtert, wie z. B. die datenschutzrechtliche Behandlung von Teleheimarbeit, besondere Formen des Mailings, aktuelle Entwicklungen im Befreiungswesen.

Am 7. November 2005 kam der AK DSB bei der GEZ in Köln zu einer außerordentlichen Sitzung zusammen. Themen waren u. a. die gemeinsame Stellungnahme zum Bericht der vier Landesdatenschutzbeauftragten über ihre GEZ-Prüfung und die geplante Betriebsstättendatenbank bei der GEZ.

Art. 29 Abs. 2 der EU-Datenschutzrichtlinie sieht die Einsetzung einer Europäischen Datenschutzgruppe vor, die aus Vertretern der einzelnen Mitgliedstaaten der EU besteht. Unter dem Vorsitz des Bundesbeauftragten für den Datenschutz, Herrn Peter Schaar, berät sie die EU-Kommission und trägt zur einheitlichen Anwendung der Datenschutzrichtlinien der EU-Staaten bei. Seit Ende 2001 ist ein Vertreter des AK DSB, der Datenschutzbeauftragte des NDR, Herr Maximilian Merten, an der Arbeit der Gruppe beteiligt.

Dadurch ist eine regelmäßige Information der Rundfunkanstalten über sich abzeichnende Entwicklungen und Meinungsbildung im Bereich des Datenschutzes auf Europäischer Ebene sichergestellt.

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.

Zur Vereinheitlichung der Sicherheitsstandards unter den Nutzern des CN wurde ein IT-Sicherheitsgremium gegründet, dem ich als Vertreterin des AK DSB als beratendes Mitglied angehöre.

Im Berichtszeitraum haben zwei Sitzungen des IT-Sicherheitsgremiums für das ARD CN stattgefunden.

Auf der Sitzung am 12. Oktober 2005 beim NDR in Hamburg hat sich das Gremium eine Geschäftsordnung gegeben. Es wurden Mustervereinbarungen zur Datensicherheit beschlossen, die jeder Nutzer des CN unterschreiben muss. Neben vielen anderen Themen wurde der Umgang mit IT-Sicherheitsvorfällen diskutiert. Auf der Sitzung am 8. Februar 2006 wurden wir über den Stand der Realisierung einer Dokumentationsplattform des IT-Sicherheitsgremiums informiert. Außerdem haben wir uns mit den Verfahren für die Freigabe neuer CN-Anwendungen und mit diversen IT-Projekten der ARD beschäftigt.

Berlin, 19. Mai 2006

gez. Anke Naujock